Symantec™ Client Management Suite 7.5 powered by Altiris™ technology User Guide for Mac Management

Symantec™ Client Management Suite 7.5 powered by Altiris™ technology User Guide for Mac Management

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version:

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, , Altiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Licensed Software does not alter any rights or obligations you may have under those open source or free software licenses. For more information on the Third Party Programs, please see the Third Party Notice document for this Symantec product that may be available at http://www.symantec.com/about/profile/policies/eulas/, the Third Party Legal Notice Appendix that may be included with this Documentation and/or Third Party Legal Notice ReadMe File that may accompany this Symantec product.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release,

performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Technical Support 4

Chapter 1 Introducing the Mac in Altiris Client Management Suite 7.5 from Symantec 12

About managing Macs with CMS 12
Key CMS Mac capabilities and limitations compared to Windows 12
About supported package-delivery formats for software distribution 14

Chapter 2 Discovering Mac computers on the network 17

Discovering Mac computers 17
Creating Network Discovery tasks using the wizard 18
Manually creating and modifying Network Discovery tasks 19

Chapter 3 Installing the Symantec Management Agent and plug-ins for Mac 21

About installing the Symantec Management Agent for UNIX, Linux, or Mac 21
About agent registration 22
About the Mac Terminal and Secure Shell (SSH) 22
Symantec Management Agent for Mac installation prerequisites 23
Installing Symantec Management Agent for Mac 26
Creating a CSV file for importing Mac computers 28
Selecting Mac computers for a Symantec Management Agent pull installation 30
Creating an agent registration policy 31
Allowing incoming connections through SSH 33
Setting up Notification Server name resolution with Mac computers 34
Disabling or configuring a built-in Mac OS X firewall 35
Specifying the Symantec Management Agent for Mac installation settings 38

Installing Symantec Management Agent to the Mac OS X client computer 39
Installing the Symantec Management Agent for Mac with a push 40
Installing the Symantec Management Agent for Mac with a pull 43
Checking the agent installation 44
Viewing and managing the agent registration status 44
About solution plug-ins for Mac 48
Command-line options for managing Mac client computers 48
Installation Settings: Connection and Authentication tab 49
Try connect by SSH using SSH Key authorization settings 50
Try connect by SSH using password authorization settings 50
Login and password settings 51
Timeout settings 52
Platform detection settings 53
Installation Settings: Agent Settings tab for Mac computers 53
Installation Settings: Install XML tab 55

Chapter 4 Configuring the Symantec Management Agent for Mac 56

About configuring the Symantec Management Agent for Mac 56
Configuring the global agent settings for Mac 57
Configuring the targeted agent settings for Mac 58
Configuring maintenance window policies for managed Mac computers 60

Chapter 5 Gathering inventory from Macs 64

About Inventory Solution 65
Gathering inventory on managed computers 66
Methods for gathering inventory 67
Installing the Inventory Plug-in 69
Manually installing the Inventory Plug-in on managed Mac computers 70
Checking the deployment of the Inventory Plug-in to the managed Mac computers 71
Gathering inventory with predefined policies 72
Creating and configuring inventory policies and tasks 74
Ensuring that the managed Mac computers can receive the inventory policy 75
Checking the inventory policies on managed Mac computers 76
Gathering custom inventory 76

Creating and customizing a data class 77
Creating a custom inventory script task 78
Configuring the custom inventory sample script for UNIX, Linux, and Mac 80
About software inventory using the `filescan.rule` file 82
Gathering software inventory on managed computers using the `filescan.rule` file 82
Scanning for files on managed Mac computers using a custom file scan rule 83
Viewing inventory data in reports 84
Viewing inventory data in the Resource Manager 85
Troubleshooting problems with Inventory Solution on managed Mac computers 86
Enabling devnote logging on Mac computers 87
Troubleshooting the connection to Task Server on managed Mac computers 87

Chapter 6 Software Management Solution for Mac 89

About delivering Mac software with Software Management Solution 90
Components of Software Management Solution specific to Mac computers 90
What you can do with Software Management Solution on Mac computers 91
Implementing Software Management Solution on Mac computers 92
About Software Management Solution settings for Mac computers 93
Installing Mac profiles using Software Management Solution 94
About software policy remediation on Mac computers 95
About the Software Portal 96
Methods for delivering software to Mac computers 96
Advanced delivery actions that Managed Software Delivery can perform with Mac computers 99
Creating a Managed Software Delivery policy with the Managed Software Delivery wizard for Mac computers 100
About using tasks to manage Mac computers 101
Configuring a software delivery task for Mac computers 102
Creating a DMG file to deliver software to Mac OS X computers 104
Creating an Installer Shell script to deliver software to Mac OS X computers 105

Importing an installer into the Software Catalog to deliver software to Mac OS X computers 105
Creating a task to disable the Product Improvement pop-up 107
Creating a Managed Software Delivery policy to deliver software to Mac OS X computers 108

Chapter 7 Using Patch Management Solution for Mac 111

About Patch Management Solution for Mac 111
Implementing Patch Management Solution for Mac 112
About how Mac patching works 113
About hosting an internal SUS to obtain internal software updates 113
About patching Mac software 114
Checking for available software updates 114
Viewing the list of available software updates 115
Redirecting a Mac client computer to a local SUS 116
About the Mac compliance Dashboard 119
Viewing reports 119
Patch management for Mac return codes 120

Chapter 8 Imaging and Deploying Mac computers 122

About supporting Macintosh computers 122
Prerequisites for Mac computer setup 124
Launching Symantec's Mac pre-OS Creation Utility 125
About Symantec's Mac pre-OS Creation Utility 126
Creating and modifying NetBoot images 127
Creating and modifying NetInstall images 129
Configuring NBS for Mac computers 130
About NBS General Settings 133
Installing Network Boot Service on site server 133
Creating preboot configuration for Mac 134
Adding or importing predefined computers 135
Booting Mac computers with NetBoot image 138
Creating a Boot To task 140
Booting an unknown Mac computer in NetBoot environment 143
Booting a predefined Mac computer in NetBoot environment 146
Booting a managed Mac computer in NetBoot environment 149
Installing Mac OS using Deployment Solution 152
About Mac configuration file 155
Installing Mac OS on an unknown computer 156
Installing Mac OS on a predefined Mac computer 159
Installing Mac OS on a managed computer 163

Creating and deploying Mac images 165
Setting up automation environment on Mac computers 167
Creating a Mac image 168
Deploying a Mac image 170

Appendix A Troubleshooting 175

About Symantec Notification Manager 175
Installing the Symantec Management Agent for Mac 175
Launching the Symantec Management Agent for Mac GUI 176
Using the Symantec Management Agent for Mac GUI 176

Index 181

Chapter 1

Introducing the Mac in Altiris Client Management Suite 7.5 from Symantec

This chapter includes the following topics:

- About managing Macs with CMS

About managing Macs with CMS

You can manage Mac client computers with Client Management Suite from Symantec.

You can do the following:

- Discover Mac computers
- Install the management agent on Mac computers
- Gather hardware inventory, software inventory, and custom inventory from Mac computers
- Manage software, and deliver software to Mac computers
- Enforce security updates on Mac computers.
- Image and deploy Mac computers.

Key CMS Mac capabilities and limitations compared to Windows

Altiris Client Management Suite (CMS) 7.5 from Symantec was designed with Windows and Mac computers in mind.

See “About managing Macs with CMS” on page 12.

Most Windows capabilities are also offered for Mac computers. One example is that you discover and manage Mac computers in much the same way that you discover and manage Windows computers. Noticeable limitations are listed because they are to be resolved in a future release.

In the table, Yes in the Mac or Windows column indicates that the capability exists for that platform. Some Mac capabilities are not applicable to the Windows platform, and this condition is marked in the table as N/A.

Table 1-1 Comparison of key CMS Mac capabilities and limitations with Windows

CMS capability	Mac OS X	Windows
Network Discovery	Yes	Yes
NetBoot Imaging	Yes	N/A
Hardware, software, and user inventory	Yes	Yes
Software delivery	Yes	Yes
Platform-specific agent UI	Yes	Yes
Agent UI is localized	Future release	Yes
Intelligent software management	Yes	Yes
Software detection rules See "About delivering Mac software with Software Management Solution" on page 90.	Yes	Yes
Application metering	Future release	Yes
Self-service Software Portal (IE, Firefox, and Safari)	Yes	Yes
Remote control (pcAnywhere)	Yes	Yes
Automated software updates (Patch Management Solution)	Yes	Yes
Advanced software inventory	Yes	Yes
Custom inventory	Yes	Yes
Cross-platform reporting	Yes	Yes
Power control (Wake Up, Log Off, Restart, Shut Down)	Yes	Yes
Native DMG file support	Yes	N/A

You should also be aware that Deployment-Solution-equivalent functions such as copy file are not yet offered for managing Mac computers in CMS.

About supported package-delivery formats for software distribution

Apple extensions for software packaging and distribution can complicate some Symantec Management Platform tasks that are carried out by Notification Server.

See "About managing Macs with CMS" on page 12.

The Apple Mac OS X GUI presentation of DMG, PKG, MPKG, and APP extensions can introduce confusion for you and other Windows administrators. Confusion can arise particularly when you need to manage Mac OS X software from Notification Server: Perform transfer tasks, software import tasks, and software delivery tasks with a software push initiated from an OS other than Mac OS X.

However, Notification Server has built-in functionality to import software for Mac OS X in its repository. From that repository you can schedule distribution of the software through Quick Delivery, a Managed Software Delivery policy, or an offline task.

This topic describes the packaged software presentation under Mac OS X. It explains how DMG, PKG, MPKG, and APP files and directory extensions do and do not relate to Windows file formats and extensions. This information helps you understand how Symantec solutions and the agent platform support Apple software distribution.

Software Management Solution in Altiris Client Management Suite 7.5 from Symantec supports the following delivery media for Mac computers:

- Apple Disk Image: DMG
  A DMG is an archive similar to a Windows ISO
- Installation packages: PKG and MPKG
  These installation packages are most closely related to Windows MSI files.
- Application bundles: APP
  Mac application bundles have no Windows equivalent.

Table 1-2

Windows file formats	Related Mac file formats
ISO	DMG Mac OS X files with ".dmg" extension are Mac OS X disk image files (DMGs). A DMG is a Mac OS X proprietary format CD/DVD ROM image. A DMG is similar to an ISO file and to Apple CDR files. It represents an upgrade to Mac legacy IMG files. To store Mac software on the Windows NTFS file system, Symantec requires that you first compress the software application files into an Apple DMG. You can create a DMG using utilities that are bundled with Mac OS X. One such example is Disk Utility. After the application is compressed into a DMG, you mount the DMG on a Mac in the same way you mount a CD-ROM drive. The key DMG characteristics or features that are not available in ISO are as follows: ■ Are in over-the-Internet distribution form for Mac OS X software. ■ Behave like disk volumes. ■ Can be mounted to a mount point on Mac OS X. ■ May contain multiple partitions with Apple's proprietary HFS+ filesystem. ■ Are convertible to ISO images using Mac OS X Disk Utility. The key DMG characteristics or features that set it apart from ISO are as follows: ■ Preserves the extended attributes of the packaged software. ■ Allows secure password protection. ■ Allows encryption. ■ Allows compression. ■ Can be an image of an optical disc. The actual HDD ISO 9660 is primarily used for optical disc imaging. ■ Apple-proprietary format specific to Mac OS X. ISO 9660 is a cross-platform non-proprietary standard. DMG files are regular files and are presented that way in Finder. The power of DMG files is that they can be transferred between various operating systems, preserving all the attributes of the enclosed application or data.

Table 1-2 *(continued)*

Windows file formats	Related Mac file formats
MSI	PKG A PKG is an Apple installation package. This package can be a file package with the .pkg extension or a file package with the .mpkg extension. Installation packages contain products or product components. The products or components are known as the package payload. The installation package also contains the installation information that the Installer application and the Remote Desktop use to place product files on a file system. A PKG can be a file or a folder.
MSI	MPKG An MPKG is an Apple metapackage. A metapackage is an installation package that contains other installation packages. These other installation packages are usually component packages. A metapackage delivers the products that include multiple components. The metapackage gives users the installation options that let them select the components to install. You can combine multiple packages into a metapackage. Before you transfer one or more metapackages to another Mac, Windows, or other computer, you must roll it into an archive. You must roll metapackages into an archive to preserve the directory structure, permissions, and other attributes during the transfer. Archives include TAR, ZIP, TAR.GZ, or TAR.Z. An MPKG can be a file or a folder.
	APP Application bundles do not have a Windows equivalent.

Chapter 2

Discovering Mac computers on the network

This chapter includes the following topics:

- Discovering Mac computers

Discovering Mac computers

Network Discovery is basically the same for all platforms. The exception with Mac computers is that to discover them as computer resources, you must enable SNMP before running Network Discovery.

You can discover all the devices on your network and enter those devices in the CMDB. This process guides you through the steps to discover network devices.

Table 2-1 Process for discovering Mac devices

Step	Action	Description
Step 1	Create a Network Discovery task.	You can create and schedule a task to discover either a single device or multiple devices on a network. You can use two methods for creating tasks: using the Network Discovery wizard or creating tasks manually. See "Creating Network Discovery tasks using the wizard" on page 18. See "Manually creating and modifying Network Discovery tasks" on page 19.

Table 2-1 Process for discovering Mac devices *(continued)*

Step	Action	Description
Step 2	(Optional) Modify task settings or schedules.	After you create a Network Discovery task, you can modify the task settings or add additional schedules. See "Manually creating and modifying Network Discovery tasks" on page 19.
Step 3	View discovery data.	You can view the status of Network Discovery tasks and view reports that show discovery results. Press **F5** to refresh the page and view the status.
Step 4	Classify unknown devices.	If you have devices with an unknown classification, you can modify the SNMP classifications list. For details, please see Symantec knowledge base article TECH155182 titled "Devices are note being identified properly / classified as 'Unknown'."

Creating Network Discovery tasks using the wizard

The Network Discovery wizard is an administrator tool that guides you through creating a discovery task and configuring settings. You can later edit the task's advanced settings and schedules by editing the task.

Ensure that you have enabled SNMP before you begin.

For more information on how to enable SNMP refer to http://technet.microsoft.com/en-us/library/cc738071(v=ws.10).aspx.

This task is a step in the process for discovering Mac computers.

See "Discovering Mac computers" on page 17.

To create Network Discovery tasks using the Network Discovery wizard

1. In Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Network Discovery**.
2. On the **Network Discovery Home** page, in the **Network Discovery Quick Start Actions** Web part, click **Launch Discovery Wizard**.
3. In the wizard, on the **Step 1 Choose method of device discovery** panel, select a discovery method, and then click **Next**.
4. On the **Step 2 Enter network IP Ranges** panel, specify the portions of the network to discover, and then click **Next**.

5 On the **Step 3 Select device communication profile** panel, select a connection profile, and then click **Next**.

Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile.

6 On the **Step 4 Enter task name** panel, give the task a name, and then click **Next**.

7 On the **Step 5 Choose when to run the discovery** panel, specify the schedule of the task, and then click **Finish**.

You can view the tasks that the discovery wizard creates, on the **Network Discovery Home** page, in the **Network Discovery Task Management** Web part. You may need to click **Refresh** icon to view newly created tasks.

Manually creating and modifying Network Discovery tasks

You can manually create and modify tasks from the Task Management Portal. This option lets you configure advanced options and schedules.

When you create tasks manually, you can discover a network or an individual device.

This task is a step in the process for discovering Mac computers.

See "Discovering Mac computers" on page 17.

To manually create a task to discover a network

1 In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Network Discovery**.

2 On the **Network Discovery Home** page, in the **Network Discovery Task Management** Web part, on the **Available Tasks** tab, click **New**.

3 In the **Create Discovery Task** dialog box, specify the settings of the discovery task and click **OK**.

Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile .

To configure the maximum number of devices to discover concurrently, click **Advanced**.

4 On the **Network Discovery Home** page, in the **Network Discovery Task Management** Web part, on the **Available Tasks** tab, click the task, and then click **Schedule** to schedule it.

To manually create a task to discover a single device

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand the appropriate folder, right-click it and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Discover Device**.
4. In the right pane, give the task a unique and a descriptive name, select the connection profile, and then click **OK**.

   Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile.
5. In the task window that opens, click **New Schedule**.
6. In the **New Schedule** dialog box, specify the schedule of the task and the device that you want to discover by entering the IP address or name, and then click **Schedule**.

To modify Network Discovery tasks

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Network Discovery**.
2. On the **Network Discovery Home** page, in the **Network Discovery Task Management** Web part, on the **Available Tasks** tab, click the task, and then on the toolbar click **Edit**.

To stop Network Discovery tasks

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Network Discovery**.
2. On the **Network Discovery Home** page, in the **Network Discovery Task Management** Web part, on the **Task Runs** tab, click the task, and then on the toolbar click **Stop**.

Chapter 3

Installing the Symantec Management Agent and plug-ins for Mac

This chapter includes the following topics:

- About installing the Symantec Management Agent for UNIX, Linux, or Mac
- About agent registration
- About the Mac Terminal and Secure Shell (SSH)
- Symantec Management Agent for Mac installation prerequisites
- Installing Symantec Management Agent for Mac
- About solution plug-ins for Mac
- Command-line options for managing Mac client computers
- Installation Settings: Connection and Authentication tab
- Installation Settings: Agent Settings tab for Mac computers
- Installation Settings: Install XML tab

About installing the Symantec Management Agent for UNIX, Linux, or Mac

In the context of managing Mac computers in Client Management Suite, installation refers to installing the Symantec Management Agent for UNIX, Linux, or Mac. This ULM agent is a unified agent that runs on the UNIX-based operating systems. In

the Symantec Management Console, this agent is labeled **Symantec Management Agent for UNIX, Linux, or Mac**. In documentation referring to managing Mac computers, it is commonly referred to as Symantec Management Agent for Mac or as Symantec Management Agent.

See "About managing Macs with CMS" on page 12.

In Symantec Management Console, Symantec Management Agent for UNIX, Linux, or Mac is one of your installation options.

Installing Symantec Management Agent for UNIX, Linux, or Mac is different in some ways from installing the Windows agent. Refer to the installation prerequisites and the installation process table for details.

See "Symantec Management Agent for Mac installation prerequisites" on page 23.

See "Installing Symantec Management Agent for Mac" on page 26.

About agent registration

The agent registration feature requires a client computer to be allowed to communicate with Notification Server before it can be managed by this Notification Server. The default agent registration policy allows all computers to communicate with Notification Server. However, you can create custom agent registration policies that allow or block certain computers.

See "Creating an agent registration policy" on page 31.

After the agent registration policy allows or blocks a computer, you can only change its status manually on the **Agent Registration Status** report page. For example, you can allow or block the computers that are in the pending state. You can also revoke the registration of the agents that you have previously allowed.

See "Viewing and managing the agent registration status" on page 44.

Agent registration is supported on Windows, UNIX, Linux, and Mac platforms.

About the Mac Terminal and Secure Shell (SSH)

You can run terminal commands at the Mac Terminal, which is on the physical client computer. Using the terminal app on a Mac client computer is equivalent to opening a DOS prompt on a Windows client computer. If you do not have access to the physical computer, you can perform "Terminal" commands on a client computer through an SSH session.

The path to the terminal application on a Mac computer is **Finder > Applications > Utilities > Terminal App**.

Refer to the following Apple documentation:

- Mac OS X 10.6 Help Allowing a remote terminal to access your computer for additional information about remote terminal access using SSH.
- Mac OS X Server Command-Line Administration for additional information about the terminal app and SSH.

See "Allowing incoming connections through SSH" on page 33.

See "Symantec Management Agent for Mac installation prerequisites" on page 23.

Symantec Management Agent for Mac installation prerequisites

Mac software runs only on the hardware that is designed to support it. In this way, system requirements for managing Mac computers are simpler than Windows.

Your computer must meet the hardware prerequisites and software prerequisites before you can install the Symantec Management Agent.

See "About installing the Symantec Management Agent for UNIX, Linux, or Mac" on page 21.

Table 3-1 Symantec Management Agent for Mac installation prerequisites

Prerequisite	Description
Operating system	Any of the following operating systems: ■ Mac OS X 10.6.x (Universal binary), 10.7.x (Universal binary), 10.8.x (Universal binary) ■ Mac OS X Server 10.6.x (Universal binary), 10.7.x (Universal binary), 10.8.x (Universal binary) Universal binary means that the operating system can run on either a PowerPC or an Intel computer.
Hard disk space	60-MB minimum for temporary installation files and 60 MB for resident installed files.
RAM	25-MB minimum.

Table 3-1 Symantec Management Agent for Mac installation prerequisites *(continued)*

Prerequisite	Description
Access rights	Symantec requires administrator account credentials to connect to the client Mac computer. After you connect to the Mac as a local administrator, you can either push or pull the agent. You push the agent automatically from Symantec Management Console or pull the agent manually, from the Mac Terminal. In CMS 7.1 and earlier, explicit root privileges were required for installing the agent. If you have upgraded to CM 7.1 SP1 or later you gain root privileges in the background when you do a push installation using the administrator account credentials. If you do a pull installation, you connect to the Mac computer as an administrator and at the Mac Terminal run the `sudo ./aex-bootstrap-macosx` command. The `sudo` command gives you the administrator privileges on the Mac computer and you can install the Symantec Management Agent. When you perform a remote installation of the agent from Symantec Management Console, you install the agent using a local administrator account. This account is required for all installation methods, including push and pull. The concept of a root directory and root user may be new if you have worked only on the Windows platform. The root user is not synonymous with the Windows administrator account. Root is a particular user on UNIX-style operating systems. It is a powerful account, and you should understand it thoroughly before you enable, disable, or use it. You can find an introduction to the concept of the root user at the Apple support site in Enabling and using the "root" user in Mac OS X and in Overview of the Altiris Agent for UNIX, Linux and Macintosh Installation Process in the Symantec Knowledge Base.

Table 3-1 Symantec Management Agent for Mac installation prerequisites *(continued)*

Prerequisite	Description
Remote SSH connections enabled, if required	Only a push installation from Symantec Management Console requires that you enable remote login through Secure Shell (SSH) on the destination Mac client computer. You enable SSH in **System Preferences** in the **Sharing** window. To enable SSH, enable **Remote Login**. **Warning:** If you plan to perform a push installation, you must also configure third-party firewalls to allow an SSH connection from Symantec Management Console to the Mac client. Use the credentials that are provided in the **Installation Settings** dialog box for the computer or computers that you select to receive the push installation from the console. The path in Symantec Management Console is **Actions > Agents/Plug-ins > Push Symantec Management Agent > Install Symantec Management Agent for UNIX, Linux and Mac > Rollout Agent for UNIX, Linux, and Mac to Computers**. The Secure Shell (SSH) gives you access from Symantec Management Console (specifically, Notification Server) to remote Mac client computers. Without SSH enabled, you cannot install the agent. With SSH enabled, you can perform bulk installations of the agent from Notification Server to multiple Mac clients. To allow an incoming SSH connection, ensure that an SSH server is running on the Mac client computer and that the firewall is configured. See "Installing Symantec Management Agent for Mac" on page 26. See "Allowing incoming connections through SSH" on page 33. **Note:** If you install through a manual process or a pull installation, you do not need to enable SSH. For a pull installation, you download `aex-bootstrap-macosx`. This self-extracting script triggers the agent installation. To use this script, you use the `sudo` prefix from the Mac Terminal. The Mac Terminal is synonymous with the Windows command line. See "Command-line options for managing Mac client computers" on page 48.
Outbound connection to Notification Server is enabled	You must configure the firewall to allow an outgoing connection to a Web port on Notification Server. See "Installing Symantec Management Agent for Mac" on page 26. See "Disabling or configuring a built-in Mac OS X firewall" on page 35. Notification Server communicates through port 80 by default through an outbound connection. The agent communicates through Notification Server through port 80 (HTTP, for browsing) or port 443 (HTTPs, secure). The agent communicates with Notification Server over HTTP or HTTPs; therefore, you must configure the firewall to allow whichever type of connection you choose to allow.

Table 3-1 Symantec Management Agent for Mac installation prerequisites *(continued)*

Prerequisite	Description
Notification Server name resolution is set up	Set up Notification Server name resolution. See "Installing Symantec Management Agent for Mac" on page 26. You can set up name resolution in one of the following ways: ■ Set up name resolution through DNS. ■ Add the host name and IP address of Notification Server to the `/etc/hosts` file on the Mac client computer. See "Setting up Notification Server name resolution with Mac computers" on page 34. See "Command-line options for managing Mac client computers" on page 48. Symantec does not recommend using the option to use only the Notification Server computer IP address. This option requires reconfiguration of the Notification Server computer codebase and snapshot settings. For details, see HOWTO3674 in the Symantec Knowledge Base.
Push-installation requirements are met	If you plan to install the agent through a push, you must remove or disable the customized prompts and the login scripts that include interactive prompts. Remember that you must also configure third-party firewalls to allow an SSH connection from Symantec Management Console to the Mac client. Use the credentials that are provided in the **Installation Settings** window when you perform a push from the console. Customized prompts can cause a push installation to fail. Customized prompts are those that are multi-lined, contain colors, contain more than 200 characters, or have been customized in any other way. Login scripts that users run cannot include interactive prompts, because the Symantec installation scripts cannot detect or respond to those interactive login scripts on Mac client computers. You do not need to discover Mac computers on your network with Network Discovery before you push the agent to those computers.

Installing Symantec Management Agent for Mac

Installing the Symantec Management Agent for Mac is a process that includes several primary tasks. Click the link in the **Description** column to learn more or follow procedures. Then, click the link back to this process table to ensure that you successfully complete each installation step.

See "About installing the Symantec Management Agent for UNIX, Linux, or Mac" on page 21.

Table 3-2 Process for installing Symantec Management Agent for Mac

Step	Action	Description
Step 1	Select the Mac computers to which you want to install the agent and plug-ins.	You have the following options for selecting computers: ■ Network Discovery ■ Manual selection by adding client host names or IP addresses ■ Active Directory Import ■ Import using a comma-separated values file. See "Creating a CSV file for importing Mac computers" on page 28. See "Selecting Mac computers for a Symantec Management Agent pull installation" on page 30.
Step 2	(Optional) Define the agent registration policies.	After you install the Symantec Management Agent, it sends out a registration request to Notification Server to establish trust between the server and the client. The default agent registration policy allows automatic registration of all agents. You can modify the default policy or create custom policies to specify more restrictive rules. See "Creating an agent registration policy" on page 31.
Step 3	Prepare the Mac client computers for agent installation.	Before you install the agent, make sure that your environment meets the prerequisites. See "Symantec Management Agent for Mac installation prerequisites" on page 23. Each Mac client computer may have a different administrator user. You must log in to each computer using the administrator credentials for that client or you get a login error. If you need help with the shell, Apple Server Admin 10.6 Help may be useful to you. You can enter the following URL without spaces if you have difficulty using the link: http://docs.info.apple.com / article.html?path=ServerAdmin / 10.6/en/xg6d3f7fe1.html. See "Allowing incoming connections through SSH" on page 33. The managed Mac must be able to resolve the Notification Server computer by name, not by IP address. The fully qualified domain name may be required. See "Setting up Notification Server name resolution with Mac computers" on page 34. See "Disabling or configuring a built-in Mac OS X firewall" on page 35.

Table 3-2 Process for installing Symantec Management Agent for Mac *(continued)*

Step	Action	Description
Step 4	Specify agent configuration settings.	You can specify agent configuration settings in the Symantec Management Console. See "Specifying the Symantec Management Agent for Mac installation settings" on page 38.
Step 5	Deploy the Mac agent.	You can install the agent as follows: ■ Push the agent from the Symantec Management Console. A console push is the most common Mac agent installation method and is the best practice. See "Installing Symantec Management Agent to the Mac OS X client computer" on page 39. ■ Pull the agent from Symantec Management Console to the client Mac computer. See "Installing the Symantec Management Agent for Mac with a pull" on page 43. ■ Use the `aex-bootstrap` command on individual components. For detailed steps, see Symantec knowledge base article HOWTO21645. See "Command-line options for managing Mac client computers" on page 48.
Step 6	On the Mac client computer, check the agent installation.	After you install the agent, the managed Mac clients are ready to receive solution plug-ins. You are not required to install plug-ins as a separate step. Solutions install their plug-ins through policies. Refer to solution-specific documentation to find out how each solution plug-in works. See "Checking the agent installation" on page 44.
Step 7	On Notification Server, view and manage the agent registration status to verify successful registration.	The **Agent Registration Status** report lets you view and manage all registration requests and completed registrations from Symantec Management Agents. See "Viewing and managing the agent registration status" on page 44.

Creating a CSV file for importing Mac computers

If you want to install the Symantec Management Agent for Mac on a large number of computers, Symantec recommends that you use a CSV file. When you install the agent on the computers that require different connection and configuration settings, it is simpler to use a CSV file. Use a CSV file to import the computers and configure the installation settings.

The CSV file is a comma-delimited text file. This file includes the DNS names or the IP addresses of the client computers on which you want to install the Symantec Management Agent. Each line in the CSV file represents a computer entry that is imported into the **Symantec Management Agent Install** page. The CSV file can also contain the installation settings for each computer.

See "Selecting Mac computers for a Symantec Management Agent pull installation" on page 30.

See "Installing the Symantec Management Agent for Mac with a push" on page 40.

A CSV template file for importing UNIX, Linux, and Mac computers (`CSVTemplate.csv`) is provided with the Symantec Management Platform. The column header of the CSV template indicates the data that is required and the valid values that you can use.

Warning: The CSV file format (list separator) must meet the regional settings of the server. For example, the sample `CSVTemplate.csv` file uses the "English (United States)" regional settings with a comma "," as a list separator. You can view the Symantec Management Platform's regional settings in the Windows **Control Panel**, under **Regional and Language Options**.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To create a CSV file for importing UNIX, Linux, and Mac computers

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Symantec Management Agent**.
2. In the left pane, expand **Settings** and click **Symantec Management Agent Install**.
3. On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, under **Rollout Agent for UNIX, Linux and Mac to Computers**, right-click **CSV file template**, and then click **Save Target As**.
4. In the **Save As** dialog box, save the `CSVTemplate.csv` file in the appropriate location under a suitable name.

5 Open the new CSV file in a text editor. Enter the information for each computer on which you want to install the Symantec Management Agent for UNIX, Linux, and Mac.

You do not have to use all of the fields. You can use only the fields that you need, such as computer name, admin name, admin password, and so on.

The settings that you can specify in the CSV file are identical to the settings that you can set from the **Install Settings** window in Symantec Management Console.

6 When you have finished, save the CSV file.

Selecting Mac computers for a Symantec Management Agent pull installation

Before you can manually install the Symantec Management Agent from the **Symantec Management Agent Install** page, you need to enter or select the appropriate computers. You can select the computers that have been discovered with Network Discovery. If you prefer, you can enter the computer names manually or import the computers through Active Directory or from a CSV file.

The CSV file is a comma-separated value (comma-delimited) text file. The file includes the DNS names or the IP addresses and administrator credentials of the client computers on which you want to install Symantec Management Agent. A template for the CSV file is located in the UNIX/Linux/Mac push installation screen.

For Mac computers, each line in the CSV file represents a computer entry that is imported into the **Symantec Management Agent Install** page. You can also include the appropriate installation settings in the CSV file. These installation settings let you configure the communication and the authentication settings for the Symantec Management Agent for Mac.

Note: If you have a large number of computers that require different connection and configuration settings, use a CSV file to import the computers.

See "Creating a CSV file for importing Mac computers" on page 28.

You can select Mac computers for a manual Symantec Management Agent installation. With this type of installation, you download files and execute them on the client computer.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To select Mac computers for a Symantec Management Agent manual installation

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Symantec Management Agent**.
2. In the left pane, expand **Settings**, and then click **Symantec Management Agent Install**.
3. On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, highlight the computers to which you want to roll out the agent, as follows:

To manually add a computer	In the text box, type the computer name (which must be a DNS-resolvable name) or IP address and then click **Add**.
To select from the available computers	Click **Select Computers** and then, in the **Select Computers** window, select the appropriate computers.
To import computers from a CSV file	1 In the toolbar, click **Import computers from a selected file**. 2 In the **Select file to import** dialog, select the appropriate CSV file, and then click **Open** See "Creating a CSV file for importing Mac computers" on page 28.

4. Click **Installation Settings**, and specify the settings.
5. Verify that each computer meets the Symantec Management Agent installation prerequisites.

   See "Symantec Management Agent for Mac installation prerequisites" on page 23.

Creating an agent registration policy

Agent registration policies let you automate the agent registration process. An agent registration policy is a set of rules that determine how the incoming registration requests are processed. In the registration request content, Symantec Management Agent sends its host name, MAC address, IP address, FQDN, and logged on user data. The agent registration policy uses the registration request data and the rules that you define within the policy to decide if the request is allowed or blocked.

Warning: The default agent registration policy automatically allows all agents to communicate with Notification Server. You can modify the default policy or create custom policies to restrict the agents that can communicate with Notification Server. If no active policies are available, the status of each incoming registration request is set to pending.

You can view the registration requests in the **Agent Registration Status** report. You can access this report in the Symantec Management Console, under **Reports > Notification Server Management > Registration**.

See "Viewing and managing the agent registration status" on page 44.

To create an agent registration policy

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Agents/Plug-ins > Symantec Management Agent > Settings**.
3. Right-click **Registration Policies**, and then click **New > Registration Policy**.
4. On the right pane, specify the settings of the agent registration policy as follows:

Rules

Lets you define different types of masks for agent identification using the request data. For example, you can define a host name mask, an IP address mask, and a logged on user name mask.

A single policy can contain unlimited number of masks of any type. During the mask matching process, Notification Server treats different mask types as logical AND operation and similar mask types as logical OR operation.

For example, a policy with the following masks allows registration of all agents that have the name that matches mask "*test" and their IP address is either 10.31.12.1, 10.31.12.2, or any from 255 IP addresses from the 10.31.15.0 subnet:

- Host = *test
- IP=10.31.12.1
- IP=10.31.12.2
- IP=10.31.15.0/24

Note: Asterisk is accepted for all rules except for **IP address**. If you want to specify an IP range in a rule, you must define it with the subnet mask. For example, instead of typing **10.31.15.***, you enter **10.31.15.0/24**.

Actions

Lets you define the rule for complied agent processing with the following options:

- **Allow**
  The agents are automatically registered and you do not need to accept them manually.
- **Block**
  Requests from these agents are declined.

Note that if two policies are applicable to a registration request, and one of them allows registration and the other blocks it, the blocking policy is applied to the request.

5 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

6 Click **Save changes**.

Allowing incoming connections through SSH

After you have either disabled or configured the firewall to allow incoming and outgoing communication, you must verify connections.

Specifically, you must verify that the Mac OS X computer allows incoming connections through the SSH protocol. The Apple Mac OS X operating system has SSH installed by default, but the SSH daemon is not enabled automatically. This means that a user cannot log in remotely until you enable it.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See “Installing Symantec Management Agent for Mac” on page 26.

To allow incoming connections through SSH

1. On the client Mac, in **System Preferences**, under **Internet & Networking**, click **Sharing**.
2. In the list that appears, check **Remote Login**.
3. The SSH daemon starts immediately, and you can log in remotely using your user name.

   The **Sharing** window shows the name and IP address to use. You can also find this information by entering the following commands at the Terminal:

   `whoami` and `ifconfig`

Note: If the Mac client is located some distance from the platform server where you normally work, you have an alternative. You can work through an SSH session with the client Mac after you enable the SSH connection. You can use any SSH connection tool to enable and establish an SSH connection. One such tool is PuTTY. You can then perform actions on the Mac client computer through the SSH session instead of from the Mac terminal.

Setting up Notification Server name resolution with Mac computers

A prerequisite for installing Symantec Management Agent on Mac client computers is to set up Notification Server name resolution.

See "Symantec Management Agent for Mac installation prerequisites" on page 23.

One way to set up name resolution is to add the Notification Server computer host name and IP address to the `/etc/hosts` file on the Mac client computer.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To set up Notification Server name resolution with Mac computers

1. As an admin user, on the Mac client computer open Terminal.app.

   If you have opened a remote SSH session from Symantec Management Console, start this procedure with the next step.
2. At the command line, enter **`sudo vi /etc/hosts`**.
3. At the prompt, enter the current admin user's password.
4. When the file contents appear, press the Down-arrow key or the lowercase **j** key until you reach the last line of the document.

5 Press the lower-case letter **o** key to open a new line below the line that the cursor is on.

This action opens the **insert/edit**mode.

6 On the new line in the **insert/edit** mode, enter the Notification Server computer IP address and the Fully Qualified Domain Name (FQDN) of the Symantec Management Platform server.

If you prefer, you can enter the short name or other alias for the Symantec Management Platform server on this same line.

7 Press **Esc** to exit **insert/edit** mode.

8 Press the **colon (:)** key.

9 At the **:** prompt at the bottom of the screen, enter the lowercase letters `wq` to write the file to disk and exit the vi editor.

10 At the shell prompt, enter `cat /etc/hosts` to review the entry that you added.

Note: If you need information about the vi editor or how to use it, you can find many sources of good information on the Web.

Disabling or configuring a built-in Mac OS X firewall

For a push installation to a Mac client computer, you must disable or configure the firewall. If you do not disable the firewall, you must configure it to allow incoming and outgoing connections to and from Symantec Management Console.

When you enabled a Secure Shell (SSH) for push installations, you also should have configured third-party firewalls to allow an SSH connection from Symantec Management Console to the Mac client. Disable the third-party firewalls as well. When you re-enable SSH, re-enable the third-party firewalls.

Warning: You must disable the firewall or configure it to allow communication with the console. Otherwise, you cannot install Symantec Management Agent and plug-ins.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See “Installing Symantec Management Agent for Mac” on page 26.

The following information about ports and protocols is from Ports and Protocols for Symantec Management Platform 7.0.

Relevant information for configuring a Mac OS X firewall is shown in the following tables:

Table 3-3 Notification Server ports

Component	Port	Protocol
Notification Server	1024-65536 Default = 52028	TCP/IP
Notification Server	1024-65536 Default = 52029	TCP/IP Multicast
Agent	80	HTTP

Initial connection of Notification Server to client uses the following port:

- TCP 445 (MS DS/CIFS)

Initial connection of the client to Notification Server (after Service Starts) uses the following port:

- TCP 80 (HTTP) client download

Use the following ports for various services:

HTTP Client / Server communications, such as policy updates and posting events	The Agent establishes a connection to server port TCP 80 for HTTP and server port TCP 443 for SSL. This port is configurable by the user and can be set to any free port.
Downloading packages from Notification Server	Clients can download through HTTP.
Wake on LAN and Power Management	The default port is 52028.
To access Symantec Management Console using a remote computer	Notification Server uses HTTP (port 80) to connect to the server and download the client application or console content.

To communicate with Symantec Management Agent on the Mac	Notification Server uses SSH to connect to the client computer. Notification Server copies the bootstrap and then HTTP or HTTPs from the client computer to Notification Server to download the agent, as follows: ■ Initial connection of Notification Server to UNIX, Linux, or Mac client TCP 22 (SSH, configurable) ■ Initial connection of client to Notification Server (after Service Starts) TCP 80 (HTTP), 443 (HTTPS) or other custom port depending on Notification Server configuration for agent download

To disable or configure a built-in Mac OS X firewall on a Mac OS X 10.6 computer

1. On the client Mac, on the **Apple** menu, click **System Preferences...**.
2. In the **System Preferences** window, on the **View** menu, click **Security**.
3. Click the **Firewall** tab.
4. Click **Start** to enable the firewall or click **Stop** to disable it.
5. To configure the firewall click **Advanced...**.
6. The following options appear:

Block all incoming connections	This option is the strictest one.
Automatically allow signed software to receive incoming connections	Lets the digitally signed applications access your network without prompting
Enable stealth mode	Causes the computer to ignore pings and similar software that attempts to discover your computer
Plus (**+**) and minus (**-**) buttons	The buttons let you add applications to the firewall and remove applications from the firewall. When you add applications, you can either allow traffic to them or block traffic from them.

7. To save settings, click **OK**.

Specifying the Symantec Management Agent for Mac installation settings

The Symantec Management Agent installation settings are the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac. You must specify the appropriate privileged account login name and password for each target computer.

See "Installing the Symantec Management Agent for Mac with a push" on page 40.

When you import computers from a CSV file, you can specify the appropriate installation settings for each computer in the CSV file. If you do not specify any settings in the CSV file, you must specify the appropriate settings for each target computer. You must also specify the appropriate settings for each computer if you added computers manually, Specify those settings before you install the Symantec Management Agent for Mac.

You can specify installation settings for a particular computer or for multiple computers. If you select multiple computers, the same installation settings are applied to each computer. You can also clone the current installation settings from a computer and apply it to other computers.

See "Creating a CSV file for importing Mac computers" on page 28.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To specify the Symantec Management Agent installation settings

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
2. On the **Symantec Management Agent Install** page, on the **Install Symantec Management Agent for UNIX, Linux and Mac** tab, under **Rollout Agent for UNIX, Linux, and Mac to Computers**, in the computer list, select the computer for which you want to change the Symantec Management Agent installation settings, and then click **Installation settings**.

   If you want to specify identical installation settings for multiple computers, select the appropriate computers.
3. (Optional) If you want to clone the current installation settings from a particular computer, in the **Installation Settings** dialog box, in the **Load settings of** drop-down list, select the appropriate computer.

4 Specify the installation settings for the selected computers as follows:

Connection and Authentication	This tab lets you configure the communication and the authentication settings for the Symantec Management Agent for Mac push installation. See "Installation Settings: Connection and Authentication tab" on page 49.
Agent Settings	This tab lets you configure the Symantec Management Agent for Mac upgrade, configuration, and startup settings. See "Installation Settings: Agent Settings tab for Mac computers" on page 53.
Install XML	This tab displays the Symantec Management Agent for Mac upgrade, configuration, and startup settings in XML format. You can save the XML to a file and upload the file to a client computer. Then you can use it to manually install and configure the Symantec Management Agent for Mac. See "Installation Settings: Install XML tab" on page 55.

5 Click **OK**.

Installing Symantec Management Agent to the Mac OS X client computer

Deploying Symantec Management Agent is prerequisite to installing the Inventory Solution plug-in or deploying Inventory policies.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To deploy the Symantec Management Agent to the Mac OS X computer

1 In Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.

2 On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, under **Rollout Agent for UNIX, Linux and Mac to Computers**, in the text box, enter the host name or IP address, and then click **Add**.

3 Select the computer that you added, and click **Installation Settings**.

4. In the **Privileged account password** field, enter the root account password for the Mac and ensure that the remaining settings are correct.

   Note that the installation directory settings under **Agent Settings** do not apply to Mac OS X.

5. Click **OK**.

6. On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, under **Rollout Agent for UNIX, Linux and Mac to Computers**, click **Install**.

   Wait one minute to allow the agent to install.

7. On the Mac OS X computer click **Go > Utilities** to verify that the Symantec Management Agent icon is present.

8. Click **Go > Utilities > Terminal** and enter one of the following commands to check the log file:

   - `aex-helper check`
   - `aex-helper query ns`
   - `aex-helper -v`
   - `aex-sendbasicinv`

   You can run terminal commands on the physical client computer, or you can perform this step through an SSH session with the Mac client.

9. Ensure that no errors exist in the log file.

Installing the Symantec Management Agent for Mac with a push

You can push the Symantec Management Agent for Mac to any computer that is listed in the **Symantec Management Agent Install** page.

The process of the push installation of the Symantec Management Agent for Mac is as follows:

- Symantec Management Platform attempts to connect to the target computer through SSH.

  The SSH protocol supports logon with either privileged or unprivileged user accounts and multiple passwords. A privileged user has more access than an unprivileged user. Therefore, it is more secure to connect through unprivileged users. This step refers to connecting from Symantec Management Console to the client Mac through SSH. Symantec assumes that the client is configured not to allow a privileged SSH user to connect remotely.

  If you use unprivileged users, you must also specify at least one privileged user. You must use a privileged account to install the agent.

See "Symantec Management Agent for Mac installation prerequisites" on page 23.

- When a connection is established, Symantec Management Platform determines the client computer's operating system and environment. The platform then launches the appropriate platform-specific push-install script.
- The push-install script creates a directory structure on the client computer. It then attempts to download the `aex-bootstrap` utility from the Symantec Management Platform computer.
  The push-install script tries each of the following methods, in order, until one succeeds: SCP/SFTP, wget, curl.
  If all of these methods fail, the script uses `dd` command to transfer the `aex-bootstrap.Z.uu` archive to the target computer. It then uses uudecode to convert the archive to a native format.
- The `.aex-agent-install-config.xml` file, which contains all of the Symantec Management Agent installation settings, is downloaded to the client computer.
- The `aex-bootstrap` script is executed, and the SSH connection to Symantec Management Platform is closed.
- The `aex-bootstrap` script downloads the rest of the Symantec Management Agent from the Symantec Management Platform computer. It then configures the Symantec Management Agent with settings from the `.aex-agent-install-config.xml` file.
- When the Symantec Management Agent for Mac runs for the first time, it collects basic inventory and posts it to Symantec Management Platform.
- After all necessary updates are completed on the platform server, Symantec Management Agent for Mac receives tasks and policies from Symantec Management Platform.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To install the Symantec Management Agent for Mac with a push

1. Select the Mac computers on which to install the Symantec Management Agent.

   You can select multiple computers by using the Shift or Ctrl key.

   See "Selecting Mac computers for a Symantec Management Agent pull installation" on page 30.

2. If necessary, configure the appropriate installation settings.

   If you added computers manually, you must specify the appropriate installation settings for each target computer before you install the Symantec Management Agent for Mac. If you imported computers from a CSV file, you may have specified the installation settings for each computer in that file. You can change these settings for individual computers or groups of computers.

   If you configured Mac computers in the same way, such as using the same password for the root account, you can select multiple computers using the Shift or Ctrl key. When you select multiple Mac computers, you only need to define Installation Settings once. Those settings apply to all previously selected Mac computers.

   See "Specifying the Symantec Management Agent for Mac installation settings" on page 38.

3. (Optional) In the **Simultaneous Tasks** box, specify the number of installations to run simultaneously.

   This value defines the number of threads running in parallel and serving Symantec Management Agent pushing. All of the threads share a common queue from which they take the next computer to install to. The default value is 5, but you may want to use a different value. You might change the value to suit the performance of the Symantec Management Platform, the client computers, and the network capacity. Increasing the number of simultaneous tasks may reduce the total installation time.

4. Click **Install**.

   The Status column in the computer list shows the success or failure of the installation on each computer. Note that the newly installed Symantec Management Agent reports its status back to the originating Notification Server. This reporting to the originating Notification Server occurs even if a different Notification Server manages the managed computer.

5 If the computer list is not refreshed automatically, in the toolbar, click **Refresh** to view the current push installation status for each computer.

6 When the installation process is complete, view the **Installation Status** report to confirm that the agent has been installed successfully on all of the computers

The installation process can take up to 10 minutes.

Installing the Symantec Management Agent for Mac with a pull

You can pull the Symantec Management Agent to each computer if necessary. To pull the agent you must have a direct connection between Notification Server and the Mac client computer.

You might need to pull the agent in the following situations:

- SSH is not available.
- The target computers are behind a firewall.

The `bootstrap` program always downloads from Notification Server. This installation includes the download of the agent and its components and occurs from Notification Server. The agent directory contains the agent components such as task handlers. The agent installation directory contains the bootstrap binary (executable) file.

The URL of the **Download Symantec Management Agent for UNIX, Linux and Mac** page is shown on the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, under **Download Page URL for UNIX, Linux and Mac users**. You can view the page, but you cannot change this setting.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To install the Symantec Management Agent for Mac with a pull

1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.

2 On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, under **Download Page URL for UNIX, Linux and Mac users**, in the **Select platform** drop-down list, click the appropriate platform, and then copy the URL.

3 Log on to the remote computer as an administrator.

4 Ensure that the remote computer meets the Symantec Management Agent for Mac installation prerequisites.

See "Symantec Management Agent for Mac installation prerequisites" on page 23.

5 On the remote computer, open a Web browser, and then paste the URL:

http://*SMPName*/Altiris/UnixAgent/AltirisUnixAgentDownload.aspx?Id=*Platform*

SMPName is the name of your Notification Server computer and *Platform* is Mac.

6 Follow the instructions that are displayed on the **Download Symantec Management Agent for UNIX, Linux and Mac** page for downloading and running the install bootstrap program on the remote computer.

Checking the agent installation

Ensure that the agent was installed correctly.

This task is a step in the process for installing the Symantec Management Agent for Mac.

See "Installing Symantec Management Agent for Mac" on page 26.

To check the agent installation on the client computer

1 On the Mac OS X computer click **Go > Utilities** to verify that the Symantec Management Agent icon is present.

2 Click **Go > Utilities > Terminal** and enter the following command to check the log file:

```
less /opt/altiris/notification/nsagent/aex-nsclt-install.log
```

You can run terminal commands on the physical client computer, or you can perform this step through an SSH session with the Mac client.

3 Ensure that no errors exist in the log file.

To check the agent installation in the Symantec Management Console

1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.

2 On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, you can view the status of the installation process for each computer.

3 (Optional) For more detailed report, click **Status report**.

Viewing and managing the agent registration status

The **Agent Registration Status** report lets you view all registration requests and completed registrations from Symantec Management Agents.

In this report, you can see the computers that the **Agent Registration Policy** has automatically allowed or blocked. Note that for direct Symantec Management Agent push installation, the registration is bypassed. However, the computers are still displayed in the report and their status is set to **Allowed**. If no **Agent Registration Policy** applies to the computer, its status is set to **Pending** and the right-click menu lets you manually allow or block it. The right-click menu also lets you revoke the trust of the agents that you have previously allowed.

See "Creating an agent registration policy" on page 31.

Incoming registration requests are distinguished by the resource keys and they are merged based on the resource keys lookup.

In some situations, duplicate registration requests may appear. For example, if you reinstall the agent on a computer that is already registered on Notification Server, its public key changes. In this case, Symantec recommends that you approve the registration request to let this computer continue communicating with Notification Server. Also, the duplicate registration requests may appear if you have computers with identical resource keys in your network. In this case, Symantec recommends not to approve the duplicate registration request because it may cause connectivity issues for the resource that previously existed.

If you have duplicate registration requests in your report, the requests are handled as follows:

- If the initial request is allowed and the duplicate request is also allowed, the duplicate request is merged with the existing resource and the report is updated to display a single entry.
- If the initial request is allowed but the duplicate request is blocked, both requests remain in the list. The allowed request represents the actual resource and the duplicate request in blocked or pending state represents the registration attempt from a potentially duplicated resource.

The **Agent Registration Status** report keeps all requests for audit purposes and lets you continuously observe them.

To view and manage the agent registration status

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, under **Reports**, expand **Notification Server Management > Registration**, and then click **Agent Registration Status**.

3 (Optional) On the **Agent Registration Status** page, use the right-click menu options to modify the status of the agent. Note that depending on the status of the agent, the right-click options vary.

Allow

You can allow the agents that are in the **Pending**, **Blocked**, or **Revoked** state.

If you allow a blocked agent, the trust is granted next time when the agent sends a registration request to Notification Server.

Block

You can block the agents that are in the **Pending** or **Revoked** state.

If you block a revoked computer, its functional status does not change. However, changing the status lets you differentiate the revoked computers that should never again connect to Notification Server from the revoked computers that may still require your attention.

Note that computers with the **Blocked** status are removed from the list after a predefined period of time if no new registration requests were sent from the same computer during this time. The default period is three months, but you can change it on the **Purging Maintenance** page.

Revoke

You can revoke the registration of the agents that you have previously allowed. For example, you can revoke the registration for the client computer that is reported missing or stolen. After you revoke the agent, it stops receiving policies from Notification Server. Also, a revoked computer cannot be used as a site server.

During the revocation of internal agent trust, the agent encryption key registration gets marked as revoked on Notification Server. Revoked agents do not receive policies and do not run tasks. Also, the revoked agent clears locally stored policies to minimize its activity. After the revocation, Symantec Management Agent is forced to reinitiate the registration process.

The agent receives information about its revoked status next time when it tries to access secured data. Notification Server does not notify the agent about the revocation event when it occurs.

Note that the revoked agent remains in the **Revoked** state even if the agent registration policy allows it. You must manually manage the revoked computers, if you want to change their state.

About solution plug-ins for Mac

In most cases you only install Symantec Management Agent. After you install Symantec Management Agent, you enable installation policies for solutions from the console as you do with Windows computers. After that the agent on the managed Mac checks policies, and any required solution plug-ins are installed automatically. Some solution plug-ins are installed automatically through Symantec Management Agent.

See "Installing Symantec Management Agent for Mac" on page 26.

In some cases you install a plug-in. These cases are called out explicitly in the text of solution-specific documentation when you are required to install a plug-in.

Plug-in policies come with a default target (or filter) for Mac computers. You can change targets; for example, if some Mac computers on your network are servers, you can exclude them from having solution plug-ins installed.

You can download required plug-in such as plug-ins for Inventory Solution, Patch Management Solution, and Software Management Solution from Notification Server, which you access in the Symantec Management Console. If you have Notification Server and site servers, the agent on the managed Mac detects the nearest and fastest server and downloads plug-ins from there.

Command-line options for managing Mac client computers

When managing Mac client computers in the Client Management Suite, you may need to use command-line options.

See "Installing Symantec Management Agent for Mac" on page 26.

You can view a list of command-line options by executing the following commands at the Mac Terminal or through an SSH remote connection:

- `-h`
- `-help`

See "About the Mac Terminal and Secure Shell (SSH)" on page 22.

Refer to the following technical articles for details about how to use command-line options when you manage Mac client computers:

- TECH29115 titled "NS Agent for UNIX, Linux, and Mac commands and command-line parameters."
  This article presents all user-facing commands. This article was written for 6.x; however, most information applies to 7.x.

- TECH45453, titled "Client Task Agent 7.x for UNIX, Linux, and Mac command lines." Includes the `aex-cta` command.
- HOWTO36005, titled "UNIX, Linux, and Mac aex-smf command-line tool."

Installation Settings: Connection and Authentication tab

The **Connection and Authentication** tab lets you configure the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac push installation.

Warning: Do not use non-ASCII characters in file or directory names when you configure installation settings.

On the client side, SSH must allow the certificate connection, where by default only user name and password are used. The procedure for generating an SSH key is beyond the scope of this guide.

Table 3-4 Installation Settings: Connection and Authentication tab

Setting	Description
Try connect via SSH using SSH Key authorization	When you enable this option, these settings are used to establish an SSH connection to the target Mac computer using SSH key authorization. See "Try connect by SSH using SSH Key authorization settings" on page 50.
Try connect via SSH using password authorization	When you enable this option, these settings are used to establish an SSH connection to the target Mac computer. The connection is established with SSH password authorization. See "Try connect by SSH using password authorization settings" on page 50.
Login and password	These settings specify the appropriate user account credentials for SSH connections. See "Login and password settings" on page 51.
Timeout settings	These settings specify the login timeout periods and command timeout periods and the upload speed of the Symantec Management Agent package. See "Timeout settings" on page 52.
Platform detection	These settings specify whether Symantec Management Platform automatically detects the target computer's operating system or whether the target computer's operating system is defined manually. See "Platform detection settings" on page 53.

Try connect by SSH using SSH Key authorization settings

These settings are used to establish an SSH connection to the target UNIX, Linux, or Mac computer using SSH key authorization. The SSH key authorization method lets you connect to the target computer from an authorized computer without entering a user name and a password.

To use SSH key authorization, you first need to generate an SSH key. You then need to save the SSH private key on the Symantec Management Platform computer, and configure the target computer with the SSH public key. To generate an SSH key, you can use a native SSH key generator. You can also use the SSH key generation module that is provided with Symantec Management Platform.

See "Installation Settings: Connection and Authentication tab" on page 49.

Table 3-5 Try connect by SSH using SSH Key authorization settings

Setting	Description
SSH key file	The SSH private key file to use. You can type the full path and file name, or click **...** to select the appropriate file.
SSH key password	The password that is used to protect the SSH key file. If no password is configured, leave this field blank.
SSH key type	The type of SSH key encoding: RSA or DSA.
Port	The port to which the target computer's SSH server listens. Default: 22
Prompt	The target computer's logon prompt for a privileged user. Default: `%, $, #, >`

Try connect by SSH using password authorization settings

This setting specifies the port to use when the Symantec Management Platform attempts to connect to the target computer using SSH password authorization.

See "Installation Settings: Connection and Authentication tab" on page 49.

Table 3-6 Try connect by SSH using password authorization settings

Setting	Description
SSH port	The port to which target computer's SSH server listens. Default: 22

Login and password settings

These settings specify the appropriate privileged user account credentials for SSH connections. You can optionally specify multiple privileged user accounts and unprivileged user account credentials.

See "Installation Settings: Connection and Authentication tab" on page 49.

Table 3-7 Login and password settings

Setting	Description
Privileged account login	The login name of a privileged user account. A privileged user is one that has permission to install and use system programs.
Privileged account password	The password for the privileged user account that was specified previously.
Privileged account prompt	The target computer's logon prompt for a privileged user. Separate multiple values with a comma. Default: %, $, #
Use privileged account multiple password	This option lets you install the Symantec Management Agent on a group of computers that have different privileged user account names and passwords. The specified login name and password combinations are tried on each target computer until the connection succeeds. **Warning:** The passwords that you type in this section are not hidden. You need to specify the following information: ■ **Logins**: The list of privileged account login names, one entry per line. ■ **Passwords**: The corresponding list of privileged account login passwords, one entry per line. ■ **Prompts**: The target computer's logon prompt for a privileged user. Separate multiple values with a comma. Default: %, $, #

Table 3-7 Login and password settings *(continued)*

Setting	Description
Log in first using unprivileged user	This option lets you log in with an unprivileged (unauthorized) user account first. You then switch to a privileged user account. You can use this option if the target computer does not allow remote privileged user logons. Specify unauthorized user credentials or enter multiple users and passwords. You need to specify the following information: ■ **Unprivileged User Login**: The login name of an unprivileged user account. ■ **Unprivileged User Password**: The password for the privileged user account that is specified previously. ■ **Unprivileged User Prompt**: The target computer's logon prompt for an unprivileged user. Separate multiple values with a comma. Default: `%, $, #, >` **Note:** A regular unprivileged user on Mac OS X must be given permissions to SSH to the system. Otherwise, the unprivileged user may not have SSH access to the Mac OS X system to perform push install. To supply the user with SSH access, on Mac OS X go to **System Preferences > Sharing > Remote Login**. A regular unprivileged user on Mac OS X can only be used to perform a push installation through users who are allowed to administer the computer. On Mac OS X, see **System Preferences > Accounts**. Due to the implemented security on Mac OS X, unprivileged users cannot use root user to perform a push installation.
Use unprivileged user multiple passwords	This option lets you install the Symantec Management Agent on a group of computers that have different unprivileged user account names and passwords. The specified login name and password combinations are tried on each target computer until the connection succeeds. **Warning:** The passwords that you type in this section are not hidden. You need to specify the following information: ■ **Logins**: The list of unprivileged account login names, one entry per line. ■ **Passwords**: The corresponding list of unprivileged account login passwords, one entry per line. ■ **Prompts**: The target computer's logon prompt for an unprivileged user. Separate multiple values with a comma. Default: `%, $, #, >`

Timeout settings

These settings specify the login timeout periods and the command timeout periods and the upload speed of the Symantec Management Agent package.

See "Installation Settings: Connection and Authentication tab" on page 49.

Table 3-8 Timeout settings

Setting	Description
Login timeout	Specifies how long the Symantec Management Platform should wait for a successful login to the target computer. Default: 120 seconds
Command timeout	Specifies how long the Symantec Management Platform should wait for a reply from the commands that are executed during the push installation. Default: 60 seconds
Upload speed	Specifies the upload speed of the Symantec Management Agent installation package. The available values are Fast, Medium, Slow. This option affects uploading with the dd command only.

Platform detection settings

These settings specify whether the Symantec Management Platform automatically detects the target computer's operating system or whether the target computer's operating system is defined manually. If the target computer's operating system is defined manually, you need to select the appropriate value.

See "Installation Settings: Connection and Authentication tab" on page 49.

Warning: Be careful with the manual selection option if you want to configure installation settings for multiple computers.

Table 3-9 Platform detection settings

Setting	Description
Automatically discover OS type	The Symantec Management Platform detects the target computer's operating system automatically when the push installation process starts.
Manually select OS type	This drop-down list specifies the target computer operating system.

Installation Settings: Agent Settings tab for Mac computers

On the **Agent Configuration** page, the **Agent settings** tab lets you configure the Symantec Management Agent for Mac upgrade, configuration, and startup settings.

If you need to upgrade the Symantec Management Agent from an earlier version, you can choose to keep the current Symantec Management Agent settings. The Directories settings specify the directories that the Symantec Management Agent uses. The Symantec Management Agent execution settings define the behavior of the Symantec Management Agent during and after installation.

Warning: Do not use non-ASCII characters in file or directory names when you configure installation settings.

Table 3-10 Installation Settings: Agent settings tab

Setting	Description
Keep the current Agent settings if possible	If you need to upgrade the Symantec Management Agent from an earlier version, this option preserves the current Symantec Management Agent settings where applicable. Disable this option if you want to reinstall the Symantec Management Agent and configure it with the installation settings that you specify on this tab.
Installation directory	The directory where the Symantec Management Agent is installed. Default: /opt/altiris/notification/nsagent **Note:** On Mac computer, the Symantec Management Agent is always installed into the default directory.
Links directory	The directory where links to the Symantec Management Agent's executable binaries are placed. Default: /usr/bin
Directory for packages	The directory to which software delivery policies and tasks download packages. Default: %INSTDIR%/var/packages
Run Agent for Mac on startup	Specifies that the Symantec Management Agent is to run in the background each time the Mac computer starts. This setting is the default. If this setting is disabled, you must restart the agent manually every time you start the Mac client computer.
Start the Agent after installation	Specifies that the Symantec Management Agent is to start immediately after the push installation. If you disable this setting, the agent starts automatically after the next restart, but only if the **Run Agent for Mac on startup** setting is enabled.
Allow unprivileged users to run programs	Specifies that unauthorized users are allowed to run software delivery policies and tasks on the target computer.

Installation Settings: Install XML tab

The **Install XML** tab displays the Symantec Management Agent for Mac upgrade, configuration, and startup settings in XML format. You can save the XML to a file and upload the file to a client computer. You then use the file to manually install and configure the Symantec Management Agent for Mac.

If you use `aex-bootstrap` for manual agent installation, the `aex-bootstrap` looks for this XML file in the **/tmp** directory. To facilitate that process, copy the XML file as `.aex-agent-install-config.xml` to the **/tmp** directory. You can then run `aex-bootstrap` manually to use the settings that this file contains. The XML file settings override any `aex-bootstrap` command line parameters, including the specification of the Notification Server computer name.

Table 3-11 Installation Settings: Install XML tab

Setting	Description
Main display area	The main display area shows the Symantec Management Agent for Mac upgrade, configuration, and startup settings in XML format.
Save as file	This button lets you save the displayed XML to a file.

Chapter 4

Configuring the Symantec Management Agent for Mac

This chapter includes the following topics:

- About configuring the Symantec Management Agent for Mac

About configuring the Symantec Management Agent for Mac

The default Symantec Management Agent configuration settings are suitable for a small Symantec Management Platform environment, such as fewer than 1,000 nodes.

As your environment grows, or if your organization has particular requirements, you need to make the appropriate configuration changes.

The agent configuration settings are applied to the appropriate managed computers using agent configuration policies. You can modify these policies to change the settings at any time. The new configuration settings are applied to the agents when the managed computers get their next policy updates (which is typically once a day).

The Symantec Management Platform provides the following types of agent configuration policies:

Global settings	The global configuration settings apply to all Symantec Management Agents on all managed computers. These settings are applied as a single policy that automatically targets every managed computer. See "Configuring the global agent settings for Mac" on page 57.

Targeted settings	The targeted agent settings are the general parameters that control the Symantec Management Agent, including how the agent communicates with Notification Server. You can modify the default policies that are supplied with the Symantec Management Platform. You can create your own targeted agent settings policies and apply them to the appropriate managed computers. See "Configuring the targeted agent settings for Mac" on page 58.
Maintenance windows	A maintenance window is a scheduled time and duration when maintenance operations may be performed on a managed computer. A maintenance window policy defines one or more maintenance windows. You can modify the default policy that is supplied with the Symantec Management Platform. You can create your own maintenance window policies and apply them to the appropriate managed computers. See "Configuring maintenance window policies for managed Mac computers" on page 60.

The targeted settings policies and maintenance window policies are applied to the managed computers that are included in the specified policy targets. These targets may not be mutually exclusive. Two or more policies of the same type may apply to the same managed computer.

If a managed computer has two or more targeted settings policies that are applied to it, Notification Server selects the policy to use. The selection is based on the policy GUID, and is not transparent to the user. You cannot determine beforehand which policy is chosen. However, once the selection has been made, it is used consistently to ensure that the same policy is applied at every policy update.

If two or more maintenance window policies apply to the same managed computer, the policies are merged. All of the specified maintenance windows are used.

Configuring the global agent settings for Mac

The global configuration settings are set the same way on all computers. These settings apply to all Symantec Management Agents on all managed computers. The global agent settings are applied as a global agent settings policy, so they are updated in the same way as any other policy. By default, the global agent settings policy is refreshed hourly. You cannot delete or disable the global agent settings policy or create alternative versions of it.

If you want to specify agent settings for particular groups of managed computers, you need to configure the appropriate targeted agent settings policies.

See "Configuring the targeted agent settings for Mac" on page 58.

To configure the global agent settings for Mac

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Global Settings**.
2. On the **Symantec Management Agent Settings - Global** page, make the appropriate configuration settings on the following tabs:

General	Specify the Tickle/Power Management and Package Multicast settings.
Authentication	Specify the user name and password that the Symantec Management Agent uses when it connects to Notification Server or a package server. In this tab, you can also specify the remote troubleshooting password, which you can use to view agent policy information with diagnostic tools.
Events	Specify Notification Server events that you want to capture.

   For more information, click the page and then press **F1**.
3. Click **Save changes**.

Configuring the targeted agent settings for Mac

The targeted agent settings policy lets you configure the general parameters that control the Symantec Management Agent. These parameters include how the agent communicates with Notification Server . You can apply these settings to particular groups of computers. For example, some groups of computers may have different purposes, or you may want to treat servers differently from other managed computers. You can modify the default policies that are supplied with Notification Server or create your own targeted agent settings policies.

See “About configuring the Symantec Management Agent for Mac” on page 56.

The targeted agent settings policies supplied with Notification Server are as follows:

- All desktop computers (excluding site servers)
- All site servers
- All Mac OS X servers

If you want to specify some configuration settings that apply to all Symantec Management Agents on all managed computers, configure the global agent settings policy.

See “Configuring the global agent settings for Mac” on page 57.

To configure the targeted agent settings for Mac

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
2. In the left pane, do one of the following:
   - To create a new targeted agent settings policy, click **Create new**.
   - To modify an existing targeted agent settings policy, click the policy that you want to edit.
3. To set or change the policy name, click **Rename**.

   In the **Rename Item** dialog box, type the new name, and then click **OK**.

4 In the right pane, make the appropriate configuration settings on the following tabs:

General	General settings include the policy download and inventory collection frequencies, and the computers, users, or resource targets to which the policy applies.
UNIX/Linux/Mac	If the Symantec Management Agent for Mac is installed, this tab is available and provides general settings for managed Mac computers.
Downloads	Download settings control how each agent downloads packages during software deliveries. You can enable multicast downloads and configure multicast for both master sessions and client sessions. You can override these settings for individual software delivery policies and tasks. For more information, see the topics about Software Management settings in the Software Management Solution Help.
Blockouts	Blockout periods are times when all communication between the agent and Notification Server is disabled. You can set up any number of blockout periods.
User Control	The user control settings are the options that affect what the user of the managed computer can see.
Advanced	Lets you specify an alternate URL that the Symantec Management Agent can use to access Notification Server, and turn on the power management feature.

For more information, click the page and then press **F1**.

5 (Optional) To restore the policy to its default settings, click **Restore Defaults**.

6 Click **Save changes**.

Configuring maintenance window policies for managed Mac computers

A maintenance window is a scheduled time and duration when maintenance operations can be performed on a managed computer. A maintenance operation is one that has an effect like the following:

- Changes the state of a computer.

- Causes the computer to restart.
- Interferes with a user's ability to operate the computer.

Maintenance operations include installing software, installing operating system patches, or running a virus scan.

A maintenance window policy defines one or more maintenance windows and is applied to a resource target in the same way as any other policy. These policies provide the maximum flexibility for assigning maintenance windows to computers, without complicating the management of agent settings. If multiple maintenance window policies apply to a single computer, changes to the computer are permitted during any of the maintenance windows.

See "About configuring the Symantec Management Agent for Mac" on page 56.

Using maintenance windows lets you schedule maintenance work on managed computers with minimal effect on workflow and productivity. Also, you can schedule maintenance work on critical servers at different times so no two servers are ever restarted at the same time. You can schedule a maintenance window for certain times such as daily, weekly, or monthly. The maintenance window can be available indefinitely or restricted to a particular date range.

When you apply a maintenance window to a managed computer, maintenance tasks can only be carried out on them in the scheduled time period. Maintenance tasks include actions such as patches and software deliveries. Symantec Management Agents can download software delivery packages any time, but associated programs can be run only during the maintenance windows.

The Symantec Management Agent processes the policy and provides the functionality that solutions use to determine whether a maintenance window is currently open. Functionality is also provided to allow solutions to inform Notification Server that a maintenance task has been performed.

Many tasks can be combined into a single job. At times it may take longer to complete all tasks in a job than a maintenance window allows for. If the agent has already initiated a task when a maintenance window expires, the maintenance window is automatically extended until the entire job is completed.

You can create and modify the maintenance window policies that you need and apply them to the appropriate targets. The default maintenance window policy is applied to all managed computers.

To configure maintenance window policies for managed Mac computers

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Maintenance Windows**.
2. In the left pane, in the **Maintenance Windows** folder, do one of the following:

- To create a new maintenance window policy, right-click **Maintenance Window**, and then click **New > Maintenance Window**.
- To modify an existing maintenance window policy, click the policy that you want to edit.

3 In the right pane, in the **Time zone** drop-down list, select the appropriate option:

Use agent time	The times are specified without time zone information and are applied at the local time at each managed computer. Maintenance windows open and close at different times depending on the time zones of the managed computers.
Use server time	The times are specified with time zone information, where the time zone offset is that of the server's time zone where the policy is defined. The maintenance windows open simultaneously irrespective of time zones and are compensated for daylight saving. This option ensures that maintenance windows are always coordinated with the specified local time on the server where the policy is created.
Coordinate using UTC	The times are specified with time zone information, where the time zone offset is 0. The maintenance windows open simultaneously irrespective of time zones. Daylight savings time does not affect maintenance windows.

The time zone applies to all of the maintenance windows that are specified in this policy.

4 If you want the policy to take effect on a particular date, rather than as soon as it is enabled, you can set a start date. In the upper right corner, click **Advanced** and in the **Advanced Options** dialog box, set the start date and end date, and then click **OK**.

Start	The date that the policy takes effect. The policy must be enabled in the same way as any other policy. You can enable the policy at any time before or after the start date.
End	If you want the policy to be available for a limited period of time, set the appropriate end date. The policy is unavailable after this date, whether or not it is enabled. This setting is optional. If no end date is specified, the policy is available indefinitely.

5 Create the maintenance windows that you want to include in the policy.

6 In each maintenance window, under **Daily Times**, specify the start time of the maintenance window. You must also specify either the end time or the duration in the corresponding boxes.

7 Under **Repeat Schedule**, in the **Repeat every** drop-down list, select a schedule and then specify the appropriate schedule filters:

No repeat	The maintenance window is open only once, on the day that it is applied to the managed computer.
Day	The maintenance window is open every day.
Week	Specify the weekdays on which the maintenance window is open.
Month (week view)	Specify the days of the week and the weeks of the month on which the maintenance window is open.
Month (date view)	Specify the dates of the month on which the maintenance window is open.
Yearly (week view)	Specify the days of the week, the weeks of the month, and the months on which the maintenance window is open.
Year (date view)	Specify the dates of the month and the months on which the maintenance window is open.

8 Under **Applied To**, specify the maintenance window policy target.

You can select an existing organizational group, filter, or resource target. You can also select individual resources.

Details of the selected items are displayed in the grid. You can view the list by targets, resources, computers, or users, and make any necessary additions and deletions.

9 Click **Save changes**.

Chapter 5

Gathering inventory from Macs

This chapter includes the following topics:

- About Inventory Solution
- Gathering inventory on managed computers
- Methods for gathering inventory
- Installing the Inventory Plug-in
- Manually installing the Inventory Plug-in on managed Mac computers
- Checking the deployment of the Inventory Plug-in to the managed Mac computers
- Gathering inventory with predefined policies
- Creating and configuring inventory policies and tasks
- Ensuring that the managed Mac computers can receive the inventory policy
- Checking the inventory policies on managed Mac computers
- Gathering custom inventory
- Creating and customizing a data class
- Creating a custom inventory script task
- Configuring the custom inventory sample script for UNIX, Linux, and Mac
- About software inventory using the filescan.rule file
- Gathering software inventory on managed computers using the filescan.rule file

- Scanning for files on managed Mac computers using a custom file scan rule
- Viewing inventory data in reports
- Viewing inventory data in the Resource Manager
- Troubleshooting problems with Inventory Solution on managed Mac computers
- Enabling devnote logging on Mac computers
- Troubleshooting the connection to Task Server on managed Mac computers

About Inventory Solution

Inventory Solution lets you gather inventory data about computers, users, operating system, and installed software applications in your environment.

You use policies and tasks to gather inventory. The policies and tasks are easily configured and managed using a central Web console.

See "Creating and configuring inventory policies and tasks" on page 74.

Predefined inventory policies let you gather inventory with little effort.

See "Gathering inventory with predefined policies" on page 72.

The inventory data is stored in the Configuration Management Database (CMDB). The CMDB provides a central store of data that is used across the Symantec Management Platform.

You can use different methods for gathering the following types of inventory data:

Basic inventory data:	Computer name, domain, installed operating system, etc.
Standard inventory data:	Hardware and software components, file properties, etc.
Custom inventory data:	Additional data beyond the predefined data classes in Inventory Solution.

See "Methods for gathering inventory" on page 67.

Inventory Solution provides a Web-based management console, policies to alert you about critical information, and professional quality predefined or custom Web reports that let you analyze gathered inventory data. Thus Inventory Solution includes the tools that you need to transform your inventory data into useful information.

See "Viewing inventory data in reports" on page 84.

See "Viewing inventory data in the Resource Manager" on page 85.

Gathering inventory on managed computers

You can gather inventory data by running automated policies and tasks on managed computers. This method requires that you install the Symantec Management Agent and the Inventory Plug-in on target computers. The inventory policies and tasks use the Inventory Plug-in to perform the inventory scan on the target computer. The inventory data is sent to the CMDB.

Inventory policies let you gather inventory on a recurring schedule. Inventory Solution includes the predefined inventory policies that you can use to gather inventory with little effort. You can also create your own inventory policies. You can use unique policies and schedules for different kinds of inventory. For example, you can have one policy collect hardware inventory daily, and another policy collect software inventory weekly.

See "Gathering inventory with predefined policies" on page 72.

Table 5-1 Process for gathering inventory on managed computers

Step	Action	Description
Step 1	Prepare managed computers for inventory.	Target computers must be managed and have the Inventory Plug-in installed. See "Installing the Inventory Plug-in" on page 69. See "Manually installing the Inventory Plug-in on managed Mac computers" on page 70.
Step 2	Turn on an inventory policy or create an inventory policy or a task.	You need to turn on and configure a policy or a task to collect inventory. You can use an existing policy or create and configure your own policies or tasks. See "Gathering inventory with predefined policies" on page 72. See "Creating and configuring inventory policies and tasks" on page 74.
Step 3	(Optional) Configure custom inventory policy schedules.	An inventory policy with the custom schedule does not run automatically as soon as possible after the custom schedule is created and on any new computer that joins the target collection. You can configure the two custom schedules to run the policy immediately once and on a recurring schedule later.
Step 4	View inventory results.	You can view the gathered inventory data by viewing reports and data in the Resource Manager. See "Viewing inventory data in reports" on page 84. See "Viewing inventory data in the Resource Manager" on page 85.

Methods for gathering inventory

You can use different methods for gathering different types of inventory data. Each method has special features and requirements.

Table 5-2 Methods for gathering inventory

Method	Description	Features and requirements
Basic inventory	The basic inventory method is performed automatically when the Symantec Management Agent is installed on managed computers. This feature is a core function of the Symantec Management Platform and does not require any additional inventory components. Basic inventory data includes computer name, domain, installed operating system, MAC and IP address, primary user account, etc. This information is updated on a regular basis as long as the Symantec Management Agent is running on the computer.	The features are as follows: ■ Inventory data is automatically collected when the Symantec Management Agent is installed on the client computer. No other components or steps are needed. ■ Inventory data is updated at regular intervals. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. **Note:** Basic inventory data is limited in scope.

Table 5-2 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
Standard inventory on managed computers	To use this method, you must install the Inventory Plug-in on your managed computers, and then run inventory policies. The Inventory Plug-in works with the Symantec Management Agent and uses scheduled policies to gather standard inventory data that is more detailed than basic inventory. By default, standard inventory data is gathered through more than 100 predefined data classes. Standard inventory data includes the following details about client computers: ■ Hardware components, operating system, and user accounts and groups. For example, processors, memory devices, partitions, operating system versions, total swap space size, primary users, installed local accounts, membership of the local admin group, etc. ■ File properties. More detailed information about the software, such as manufacturer, version, size, etc. When the Inventory Plug-in is installed on managed computers, all inventory policies are remotely managed from the Symantec Management Console. Inventory policies can be scheduled to run at the configurable intervals that provide up-to-date data. They can also run at the times that do not affect your network performance. See "Gathering inventory on managed computers" on page 66.	The features are as follows: ■ You can gather a broad range of inventory data. ■ Inventory data is automatically collected and updated using scheduled policies and tasks. ■ You can configure policies to report only changed data (deltas) from the previous inventory. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. ■ Target computers must have the Inventory Plug-in installed. **Note:** Maintaining current inventory data can be difficult on the computers that are not regularly connected to the network.

Table 5-2 Methods for gathering inventory *(continued)*

Method	Description	Features and requirements
Custom inventory	To use the custom inventory method, you must install the Inventory Plug-in on your managed computers. This method lets you gather additional data beyond the predefined data classes in Inventory Solution. You can create the custom inventory data classes that may be unique to your environment. You then run the custom inventory scripts that collect the custom inventory data classes. See "Gathering custom inventory" on page 76.	The features are as follows: ■ You can extend the type of inventory you gather by adding the additional data classes that may be unique to your environment and are not included by default. ■ You can use a sample script task to create or configure a custom inventory script task. The requirements are as follows: ■ Target computers must be managed using the Symantec Management Agent. ■ Target computers must have the Inventory Plug-in installed. ■ You must create custom inventory data classes and include the data classes in your custom scripts. ■ You must create and run the custom inventory scripts that collect your custom inventory data classes.

Installing the Inventory Plug-in

To gather inventory data on managed computers, you must install the Inventory Plug-in on target computers. This plug-in works with the Symantec Management Agent to perform tasks on the target computers and communicate with Notification Server.

To install a plug-in, you configure the policy that installs the plug-in on target computers. You specify from Mac the group of computers on which the policy runs and when it runs. If you choose a group that contains a computer that already has the plug-in installed, the task is ignored on that computer. When the policy is turned on, the plug-in is automatically installed on any new computer that is a member of the target group.

By default, no plug-in installation policies are turned on. If you install Inventory Solution for the first time, you must manually turn on the policies to install the Inventory Plug-in.

Before performing this task, you must install the Symantec Management Agent on target computers.

You can also manually install the Inventory Plug-in on Mac computers.

See "Manually installing the Inventory Plug-in on managed Mac computers" on page 70.

This task is a step in the process for preparing managed computers for inventory.

See "Gathering inventory on managed computers" on page 66.

To install the Inventory Plug-in

1. In the **Symantec Management Console**, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, expand **Discovery and Inventory > Windows/UNIX/Linux/Mac**, and then click the policy for the plug-in that you want to install.
3. On the policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
4. On the policy page, under **Applied to**, click **Apply to**, and then choose the computers on which you want to install the plug-in.
5. On the policy page, under **Schedule**, click **Add schedule**, and then specify the time for the policy to run on target computers.
6. Click **Save changes**.

Manually installing the Inventory Plug-in on managed Mac computers

If you cannot install the Inventory Plug-in on client computers, you can work around the problem.

See "Troubleshooting problems with Inventory Solution on managed Mac computers" on page 86.

This task is a step in the process for gathering inventory on managed Mac computers.

See "Gathering inventory on managed computers" on page 66.

To manually install the Inventory plug-in on managed Mac computers

1. On the client computer, check network setting and DNS name resolving:

   ```
   /etc/resolv.conf
   ```

   ```
   /etc/hosts
   ```

2. In the GUI, click **Finder > Go > Connect to server (*Your Notification Server*\NSCap\bin\UNIX\Inventory\Mac\universal)**, and download inventory packages from the server, where *Your Notification Server* is the name of your server.

3. On the Notification Server computer, enter the following command to create a directory named **Share** in the root folder:

   ```
   mkdir share
   ```

   To mount the Inventory plug-in folder, enter the following command:

   ```
   mount_smbfs //[domain;][user[:password]@]server[/share] share
   ```

   The command looks like the following:

   ```
   mount_smbfs //USER:PASSWORD@SERVER/NScap/bin/
   unix/inventory/mac/universal share
   ```

4. From the Notification Server computer, copy **AltirisInventory.pkg.tar.gz** and **rollout.sh** to the client computer.

5. Open the folder to which you copied the files, and execute the `sh rollout.sh` command.

Checking the deployment of the Inventory Plug-in to the managed Mac computers

After you install the Symantec Management Agent and the Inventory Plug-in on your Mac computers, you can perform advanced tasks on the physical Mac client computer or through an SSH session with the Mac client computer.

See “Installing the Inventory Plug-in” on page 69.

See “Manually installing the Inventory Plug-in on managed Mac computers” on page 70.

This task is a step in the process for gathering inventory on managed Mac computers.

See “Gathering inventory on managed computers” on page 66.

To check the deployment of the Inventory Plug-in to the managed Mac computers

1. On the managed Mac computer, click **Go > Utilities > Terminal** to open the Terminal.

   You can run the Terminal commands on the physical client computer, or you can run these commands through an SSH session with the Mac client.

2. (Optional) On the Notification Server computer, on the plug-in installation page, check **Notify user when the task is available** to receive a notification when the Inventory Plug-in is delivered to the managed Mac computer and installed in the Terminal.

3. In the Terminal on the client Mac or through SSH, enter the following command to force the installation of the plug-in:

   ```
   aex-refreshpolicies
   ```

4. In the Terminal on the client Mac or through SSH, enter the following command to verify that the plug-in has been installed successfully:

   ```
   aex-helper list
   ```

   This command generates a list of installed solutions and subagents. In the Solutions section you see an entry for Inventory.

   In the Terminal on the client Mac or through SSH, to view the version of the installed Inventory plug-in, enter the following command:

   ```
   aex-inv-helper -v
   ```

   Note that if you receive the message `Command not found`, the plug-in is not installed.

   When the plug-in is installed successfully, under **Solutions** you see **Inventory**. Under **Subagents** you see **Altiris Inventory Agent**.

5. In the Terminal on the client Mac or through SSH, enter the following command:

   ```
   less /opt/altiris/notification/nsagent/aex-inventory-install.log
   ```

   This command lets you check the Inventory plug-in installation log and check the log file for errors.

Gathering inventory with predefined policies

You can use predefined inventory polices to gather inventory data. You can turn on the predefined policies and configure them according to your needs. If you want to configure predefined policies, Symantec recommends that you clone an original predefined policy and then configure the copy.

To gather inventory with policies or tasks, you must install the Inventory Plug-in on target computers.

See "Installing the Inventory Plug-in" on page 69.

See "Manually installing the Inventory Plug-in on managed Mac computers" on page 70.

This task is a step in the process for gathering inventory on managed computers.

See "Gathering inventory on managed computers" on page 66.

To turn on predefined inventory policies

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Discovery and Inventory > Inventory**, and then click the predefined inventory policy that you want to use.
3. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
4. Click **Save changes**.
5. (Optional) After you turn on an inventory policy, you can force the policy rollout by doing the following:

   In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Resource Membership Update**, and then, under **Complete update schedule**, click **Run**.

To clone and configure predefined inventory policies

1. In the **Symantec Management Console**, browse to the predefined inventory policy that you want to clone.
2. Right-click the policy, and click **Clone**.
3. Give the cloned policy a unique name, and click **OK**.
4. On the inventory policy page, configure the policy options according to your needs.
5. (Optional) Click **Advanced** to configure the data classes, policy run options, or the software inventory rules, and then click **OK**.
6. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.

7 Click **Save changes**.

8 (Optional) After you configure an inventory policy, you can force the policy rollout by doing the following:

In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Resource Membership Update**, and then, under **Complete update schedule**, click **Run**.

Creating and configuring inventory policies and tasks

You can create new inventory policies or tasks. Later, you can browse to the created policies or tasks and modify their configuration to meet your further needs.

Before you can use inventory policies or tasks, you must install the Inventory Plug-in on target computers.

See "Installing the Inventory Plug-in" on page 69.

See "Manually installing the Inventory Plug-in on managed Mac computers" on page 70.

This task is a step in the process for gathering inventory on managed computers.

See "Gathering inventory on managed computers" on page 66.

To create and configure inventory policies

1 In the **Symantec Management Console**, on the **Home** menu, click **Discovery and Inventory > Inventory**.

2 In the **Inventory Policy status** Web part, click **New**.

3 On the inventory policy page, configure the policy options according to your needs.

4 (Optional) Click **Advanced** to configure the data classes, the policy run options, or the software inventory rules, and then click **OK**.

5 Click **Applied to**, and select the resources to which you want to apply the policy.

6 On the inventory policy page, turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

7 Click **Save changes**.

8 (Optional) After you create an inventory policy, you can force the policy rollout by doing the following:

In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Resource Membership Update**, and then, under **Complete update schedule**, click **Run**.

To create and configure inventory tasks

1 In the **Symantec Management Console**, on the **Manage** menu, click **Jobs and Tasks**.

2 In the left pane, navigate to the folder where you want to create an inventory task, right-click the folder, and then click **New > Task**.

For example, to create an inventory task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.

3 In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Gather Inventory**.

4 In the right pane, give the task a descriptive name and select the types of inventory to gather.

5 (Optional) Click **Advanced** to configure the data classes, the task run options, or the software inventory rules, and then click **OK**.

6 Click **OK** to save the task.

7 On the task page, schedule the task to run on target computers.

8 Click **Save changes**.

Ensuring that the managed Mac computers can receive the inventory policy

If the managed Mac computer does not receive the inventory policy, you can work around the problem.

See "Troubleshooting problems with Inventory Solution on managed Mac computers" on page 86.

This task is a step in the process for gathering inventory on managed Mac computers.

See "Gathering inventory on managed computers" on page 66.

To ensure that the managed Mac computers can receive the inventory policy

1. Make sure that the client computer is available in the resource target.
2. To perform a client policy refresh, enter the following command:

   `aex-refreshpolicy`

   Verify the `/opt/altiris/notification/nsagent/var/policies` for the fresh policy file using the following commands:

   - `ls -latr`
   - `aex-cta list --show-all-tasks`
3. Check the scheduling of the policy.
4. Update the resource membership.

Checking the inventory policies on managed Mac computers

After you gather inventory using policies, in the Terminal on the Mac client computer or through SSH, you can enter the following commands to verify or troubleshoot:

`aex-refreshpolicies`	To force the policy to run.
`aex-cta list --show-all-tasks`	To verify that the policy is started and running.
`aex-cta list --show-all-tasks.`	After the policy is complete, to verify that it succeeded.

Gathering custom inventory

Custom inventory lets you configure the set of inventory data that is gathered and reported to the Configuration Management Database (CMDB).

Table 5-3 Process for gathering custom inventory

Step	Action	Description
Step 1	Prepare managed computers for inventory.	Target computers must be managed by Symantec Management Agent.
Step 2	Create a custom data class.	After you create a custom data class, you can add, edit, and delete its attributes.

Table 5-3 Process for gathering custom inventory *(continued)*

Step	Action	Description
Step 3	Create a task with scripting logic and schedule it to run on the managed computers.	You can create a new task, or clone an existing sample task. You can use the script that is included in the sample task or you can create your own logic. Depending on the platform, you can write the logic in JavaScript, shell script, or other scripting languages. See "Creating a custom inventory script task" on page 78.
Step 4	View custom inventory results.	You can view the gathered custom inventory data for a data class in the Resource Manager.

Creating and customizing a data class

From the Symantec Management Console, you can create a custom data class. You can add, edit, and delete attributes of the data class and you can change the position of the attribute.

See "Gathering custom inventory" on page 76.

To create and customize a data class

1. In the **Symantec Management Console**, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Manage Custom Data classes**.
3. To create a data class, do the following:
   - On the **Manage Custom Data Classes** page, click **New data class**.
   - On the **New Data Class** page, enter a name and a description for the data class and click **OK**.
     The name of the new data class must be unique.
4. To customize a data class, on the **Manage Custom Data Classes** page, in the data classes list, click the data class.

   You customize the data class by adding, editing, and deleting its attributes.
5. (Optional) To add an attribute to the data class, do the following:

- Click **Add attribute**.
- In the **Data Class Attributes** dialog box, specify the details of the attribute.
  To add an attribute that uniquely defines a row in the data class, in the **Key** drop-down list, click **Yes**. You enforce that the attribute always has a unique value that is other than NULL.
  To add an attribute that should never be empty or blank, in the **Data required** drop-down list, click **Yes**.
  If in the **Key** drop-down list, you click **Yes**, the **Data required** option is automatically set to **Yes**. You cannot change it unless in the **Key** drop-down list, you click **No**.
- Click **OK**.

6 (Optional) To edit or delete the attributes, select the attribute, and then click the **Edit** or **Delete** symbols.

7 (Optional) To let the data class store inventory of multiple objects, on the **Manage Custom Data Classes** page, check **Allow multiple rows from a single computer resource**. The data class can store the inventory of services, user accounts, files, network cards, and other objects.

8 (Optional) To specify the sequence of the attributes, on the **Manage Custom Data Classes** page, click the attribute, whose position you want to change, and then click the up arrow or down arrow.

When you report inventory values for the columns in a Notification Server Event (NSE), the attributes are identified by the column ID and not by the column name. As a result, the order of attributes in a data class must be correct.

9 Click **Save changes**.

Creating a custom inventory script task

After you have created the custom inventory data class, you create and configure a custom inventory script task that gathers the custom inventory.

To create a custom inventory script task, you can clone a sample script task and configure it with the custom data classes that you created. You can also create and configure a custom inventory script task on the **Jobs and Tasks** portal page.

When you configure your custom inventory script, you can insert tokens in the script and create or edit tokens.

See “Gathering custom inventory” on page 76.

To clone a sample custom inventory script task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, under **Jobs and Tasks**, expand **Samples > Discovery and Inventory > Inventory samples > Custom**.
3. Right-click the sample custom inventory script task, and then click **Clone**.
4. In the **Clone** dialog box, give the cloned script a descriptive name and click **OK**.
5. (Optional) Configure the sample script, and then click **Save changes**.

   See "Configuring the custom inventory sample script for UNIX, Linux, and Mac" on page 80.
6. Under **Task Status**, do one of the following:
   - To schedule the task to run on managed computers, click **New Schedule**.
   - To perform a quick run of the task on managed computers, click **Quick Run**.
7. Click **Save changes**.

To create a custom inventory script task

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder where you want to create a custom inventory script task, right-click the folder, and then click **New > Task**.

   For example, to create a task in the **Jobs and Tasks** folder, right-click **Jobs and Tasks**, and then click **New > Task**.

   To create a task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, click **Run Script**.
4. In the right pane, type a descriptive name for the task.
5. In the **Script type** drop-down list, click the script type.
6. Enter your own script or copy a sample custom inventory script to the script editor.

   To insert a token to your custom inventory script, do the following:
   - In the **Insert token** drop-down list, click the token that you want to insert.
   - Click **Insert**.

To access a sample custom inventory script, do the following:

- In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- In the left pane, under **Jobs and Tasks**, expand **Samples > Discovery and Inventory > Inventory samples > Custom**.

7 (Optional) In the **Create New Task** dialog box, in the script editor, configure the script.

See "Configuring the custom inventory sample script for UNIX, Linux, and Mac" on page 80.

8 (Optional) To configure the advanced options for running the custom inventory script task, do the following:

- Click **Advanced**, and then, on the **Script** tab, configure the options according to your needs.
- In the **Task options** tab, configure the settings for running the script task, and the maximum possible length of the script task.
- Click **OK**.

9 In the **Create New Task** dialog box, click **OK**.

10 On the **Run Script** page, under **Task Status**, do one of the following:

- To schedule the task to run on managed computers, click **New Schedule**.
- To perform a quick run of the task on managed computers, click **Quick Run**.

11 Click **Save changes**.

The next step is to wait for the client computers to receive the new task and report the results, and then view the data that is stored in the Configuration Management Database (CMDB).

Configuring the custom inventory sample script for UNIX, Linux, and Mac

The custom inventory script for UNIX, Linux, and Mac generates a text output that contains the collected inventory data in a specified format. This data is used to create the NSE and is posted into the Configuration Management Database (CMDB). The logic of creating the NSE and posting the data is hidden from the user.

When you configure the sample script, you can modify the output that the script generates.

See “Creating a custom inventory script task” on page 78.

See “Gathering custom inventory” on page 76.

To configure the custom inventory sample script for UNIX, Linux, and Mac

1. Clone or open an existing sample of the custom inventory script task.

   Do not change the first lines of the script. Make changes after the `# SCRIPT_BEGINS_HERE` label.

2. Specify the data class.

   Example:

   ```
   echo UNIX_PS_List
   ```

3. Specify the delimiters.

   Example:

   ```
   echo "Delimiters=\" \" "
   ```

4. Specify the data type and the length of each column.

   Example:

   ```
   echo string20 string20 string20 string256
   ```

5. Specify the column names.

   Example:

   ```
   echo PID Terminal Time Command
   ```

   Note that the column names are not used in 7.x custom inventory. The column names are left for backward compatibility with 6.x Inventory Solution. You can leave this line empty in 7.x but keep the `echo` command intact.

   Example:

   ```
   echo
   ```

6. Specify commands to retrieve data from system.

   Example:

   ```
   ps -ef
   ```

7. Click **Save changes**.

About software inventory using the `filescan.rule` file

Software inventory using the `filescan.rule` file lets you collect information about the installed applications on your UNIX, Linux, and Mac computers.

A file scan agent that is included in software inventory uses the `filescan.rule` file to detect the applications that are installed on your managed computers. The `filescan.rule` file contains the data sets that represent information about different applications. The file scan agent compares each data set to the actual file system data to find out whether an application is installed.

Each data set in the `filescan.rule` file consists of two lines of data. The first line is the application description data, and the second line is the matching criteria data. The application description data consists of the product name, the manufacturer, the version, and the description of the application. The matching criteria data includes a file name or the absolute path to the file that is part of the application, file size, and cyclic redundancy check (CRC). When the file scan agent finds this file in the specified directories, the associated product is reported as part of the inventory on that system.

A data set that represents information about an application in the `filescan.rule` file looks as follows:

```
product name = "Watcher" manufacturer = "Company" version = "3.24"
description = ""

file = "/opt/secret/eys/watcher" size = "45698" CRC = ""
```

A default `filescan.rule` file is included in the Inventory Plug-in installation package for each platform. It contains an example list of some common applications.

Symantec recommends that you configure the default `filescan.rule` file to include the additional applications that the software inventory should report. You can also add entries for the applications that are developed in-house.

After you configure the `filescan.rule` file, you can create a Quick Delivery task to redistribute it to all managed UNIX, Linux, and Mac computers.

Gathering software inventory on managed computers using the `filescan.rule` file

Software inventory using the `filescan.rule` file lets you collect information about the installed applications on your UNIX, Linux or Mac computers.

Symantec recommends that you customize the default `filescan.rule` file to include the additional applications that the software inventory should report. You can also add entries for the applications that are developed in-house. After you create or customize a `filescan.rule` file, you can distribute it to the client computers.

To run the software inventory using the `filescan.rule` file, you must have the Symantec Management Agent and the Inventory Plug-in installed on your client computers.

See "Installing the Inventory Plug-in" on page 69.

See "Manually installing the Inventory Plug-in on managed Mac computers" on page 70.

To gather software inventory on managed computers using the `filescan.rule` file

1. (Optional) Copy the default `filescan.rule` file from the client computer to the Notification Server computer and customize it.

   If you do not need to distribute the file widely, you can edit the file on the client Mac computer using the `vi /opt/altiris/notification/inventory/etc/filescan.rule` command.

2. (Optional) To distribute the customized `filescan.rule` file to the client computers, in the Symantec Management Console create a **Quick Delivery** task.

   Copy the `filescan.rule` file to the following folder:

   ```
   /opt/altiris/notification/inventory/etc/
   ```

   You can use the following universal path with custom installation directories:

   ```
   `aex-helper info path -s INVENTORY`/etc/
   ```

   For more information, see the topics about creating a **Quick Delivery** task in the *Software Management Solution User Guide*.

3. For the Inventory policy that gathers software inventory, ensure that the option **File properties - manufacturer, version, size, internal name, etc.** is checked.

Scanning for files on managed Mac computers using a custom file scan rule

If you want to scan separate folders for files on a local drive using file scan functionality, you create a custom file scanning rule.

This task is a step in the process for gathering inventory on managed Mac computers.

See "Gathering inventory on managed computers" on page 66.

To scan for files on managed Mac computers using a custom file scan rule

1. In the Symantec Management Console, on the **Manage** menu, click **Policies**.

   In the left pane, expand **Discovery and Inventory**, right-click **Inventory**, and then click **New > Inventory Policy**.
2. On the **New Inventory Policy** page, under **Policy Rules/Actions**, check **File properties - manufacturer, version, size, internal name, etc.**, and then click **Advanced**.
3. In the **Advanced Options** dialog box, click the **File Properties Scan Settings** tab, and then click the **Folders** tab.
4. On the **Folders** tab, under **Mac folders**, remove all default folders, and include the target folder.
5. Click **Scan sub-folders** to scan all subfolders in the parent folder, and then click the **Files** tab.
6. On the **Files** tab, remove all predefined rules if they are not required, include a new one according to your requirements, and then click **OK**.
7. On the **New Inventory Policy** page, schedule the policy run time, and select the computers to apply the policy to.
8. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
9. Click **Save changes**.

Viewing inventory data in reports

You can use a wide variety of reports to view inventory data.

See "Viewing inventory data in the Resource Manager" on page 85.

Most reports let you filter the information that you view. For example, you can also filter the report to view computers in a certain domain. You can also filter the list of computers by using wildcards.

This task is a step in the following processes:

- Gathering inventory on managed computers
  See "Gathering inventory on managed computers" on page 66.
- Gathering custom inventory
  See "Gathering custom inventory" on page 76.

To view inventory data in reports

1. In the **Symantec Management Console**, on the **Reports** menu, click **All Reports**.
2. To view inventory reports, in the left pane, under **Reports**, expand **Discovery and Inventory > Inventory**.
3. Browse the report categories, and select the report you want to view.

Viewing inventory data in the Resource Manager

You can use the Resource Manager to view all of the inventory data for a single resource. You can view the basic inventory that is gathered from all managed computers.

See "Viewing inventory data in reports" on page 84.

This task is a step in the following processes:

- Gathering inventory on managed computers
  See "Gathering inventory on managed computers" on page 66.
- Gathering custom inventory
  See "Gathering custom inventory" on page 76.

To view the inventory data for a computer in the Resource Manager

1. In the **Symantec Management Console**, on the **Manage** menu, click **Filters**.
2. In the left pane, click **Computer Filters > All Computers**.
3. In the right pane, under **Filter Membership**, right-click a computer, and then click **Resource Manager**.
4. To view the hardware summary, on the **Resource Manager** page, click **Summaries > Hardware Summary**.
5. To view the software summary, on the **Resource Manager** page, click **Summaries > Software Summary**.

To view the inventory data for a data class in the Resource Manager

1. In the Resource Manager, on the **View** menu, click **Inventory**.
2. In the central pane, click the data class on which you want to view inventory data.
3. In the right pane, click the tab that contains the information you want to view.

Troubleshooting problems with Inventory Solution on managed Mac computers

The following notifications and commands can be helpful when you troubleshoot the problems with Inventory Solution on managed Mac computers:

Verification of the successful installation of the plug-in: notification pop-up banner	The notification banner appears on the client side only if you checked the **Notify user when task is available** box before the plug-in rollout.
`aex-helper list` command	The list of objects in the agent registry lets you check if the plug-in installation succeeded.
`aex-helper check`	This command checks if the Agent is running or not.
`aex-helper query ns`	This command displays the name of the Notification Server to which the Agent is currently assigned.
`aex-helper query resource`	This command provides basic inventory data about the client computer.
`less /opt/altiris/notification/ nsagent/aex-inventory-install.log`	This command lets you view the installation log of the plug-in.
Inventory plug-in directories under **/opt/altiris/notification/inventory/…**	The directory contents are as follows: ■ ./etc/ contains config files. ■ ./bin/ contains binary files. ■ ./lib/ contains libraries. ■ ./var/ contains logs, inventory scripts, and state files.

To resolve common problems, you may need to ensure that the target Mac computer receives the inventory policy.

You can also refer to the Symantec Knowledge Base for articles about troubleshooting Inventory Solution on Macintosh computers.

See “Ensuring that the managed Mac computers can receive the inventory policy” on page 75.

To facilitate troubleshooting, you should enable devnote logging so you have adequate log files to study.

Enabling devnote logging on Mac computers

To facilitate troubleshooting, you should enable devnote logging so you have adequate log files to study.

To enable devnote logging on Mac computers

1. In the Terminal on the Mac client computer or through SSH, to set **Devnote logging level** and **Log file size on agent**, enter the following command:

   ```
   sudo aex-helper agent -s Configuration debug_level devnote
   ```

2. To set **Log file size**, enter the following command:

   ```
   sudo aex-helper agent -s Configuration debug_file_size 0
   ```

3. To set the **Backup directory for event saving**, enter the following command:

   ```
   sudo aex-helper agent -s "Event_queue" backup_dir /path_to_dir/
   ```

See "Troubleshooting problems with Inventory Solution on managed Mac computers" on page 86.

Troubleshooting the connection to Task Server on managed Mac computers

After you schedule an inventory task to run on a client computer, the Task Server triggers task execution on the client computer at specified time. If the task does not start, there may be a problem with the connection to Task Server.

See "Gathering inventory on managed computers" on page 66.

To ensure that the client computer is registered on the Task Server, in the Terminal on the Mac client computer or through SSH, enter the following command:

```
aex-cta ts
```

Below is an example of the correct output:

Task Server: *ns2.test.domain.com*

Tickle Port: *50124*

Registered: *2012-10-30 11:34:39*

Last check: *2012-10-30 14:08:33*

If there is no Task Server information returned, you can register the client computer manually. To register the client computer, in the Terminal on this computer or through SSH, enter the following command:

```
aex-cta register
```

You can also check the connection to Task Server through graphical user interface (GUI).

To check the connection to Task Server through GUI

1. On the client Mac computer, open Symantec Management Agent.
2. In the **Symantec Management Agent** dialog box, under **Task Management**, click **Client Task Agent**.
3. In the **Symantec Management Agent: Client Task Agent** dialog box, under **Connectivity**, ensure that **Task Server** name and **Status** are present.
4. (Optional) If there is no **Task Server** and **Status** information, click **Register** to register the Task Server.

Chapter 6

Software Management Solution for Mac

This chapter includes the following topics:

- About delivering Mac software with Software Management Solution
- Components of Software Management Solution specific to Mac computers
- What you can do with Software Management Solution on Mac computers
- Implementing Software Management Solution on Mac computers
- About Software Management Solution settings for Mac computers
- Installing Mac profiles using Software Management Solution
- About software policy remediation on Mac computers
- About the Software Portal
- Methods for delivering software to Mac computers
- Advanced delivery actions that Managed Software Delivery can perform with Mac computers
- Creating a Managed Software Delivery policy with the Managed Software Delivery wizard for Mac computers
- About using tasks to manage Mac computers
- Configuring a software delivery task for Mac computers

About delivering Mac software with Software Management Solution

Software Management Solution lets users directly download and install approved software or request other software.

Software Management Solution integrates with the Software Catalog and the Software Library that are part of the Symantec Management Platform. By leveraging this information, Software Management Solution ensures that the correct software gets installed, remains installed, and runs without interference from other software. This integration lets you focus on delivering the correct software instead of redefining the packages, command lines, and so on for each delivery.

Software Management Solution supports packages for the Windows, UNIX, Linux, and Mac operating systems. With few exceptions, all the functions in Software Management Solution work the same for all platforms. For example, you use the same method to create a delivery task for a Windows, UNIX, Linux, or Mac OS package.

An important exception is Software detection rules . These rules work only on the Windows platform.

See "Key CMS Mac capabilities and limitations compared to Windows" on page 12.

See "Components of Software Management Solution specific to Mac computers" on page 90.

See "What you can do with Software Management Solution on Mac computers" on page 91.

Components of Software Management Solution specific to Mac computers

The components of Software Management Solution let you deliver and manage software on client computers.

Table 6-1 Components of Software Management Solution

Component	Description
Software delivery tasks and policies	You can use any of the several methods to deliver software to client computers. The method that you use to create the task or policy depends on your delivery requirements. See "Methods for delivering software to Mac computers" on page 96.

Table 6-1 Components of Software Management Solution *(continued)*

Component	Description
Software Portal	The Software Portal is a Web-based interface that is installed on the client computers. With the Software Portal, users can request and install software with little or no administrator involvement. See "About the Software Portal" on page 96.

See "What you can do with Software Management Solution on Mac computers" on page 91.

What you can do with Software Management Solution on Mac computers

Software Management Solution lets you distribute and manage the software that is used in your organization.

Table 6-2 What you can do with Software Management Solution

Task	Description
Configure the default settings for Managed Software Delivery policies.	Configuration settings control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. Then you can change the settings for a specific policy only when needed. See "About Software Management Solution settings for Mac computers" on page 93.
Perform an advanced software delivery.	Managed Software Delivery simplifies your advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources and their dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery.
Perform a Quick Delivery of a single software resource.	You can perform a Quick Delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software.
Deliver a package without defining a software resource.	Package Delivery lets you quickly push out any package regardless of whether it is associated with a software resource.

Table 6-2 What you can do with Software Management Solution *(continued)*

Task	Description
Deliver the tasks and packages that were created in Altiris Software Delivery Solution 6.x.	When you upgrade from Notification Server 6.x to Symantec Management Platform 7.x, you can migrate your software-related tasks and packages.
Deliver software to fulfill user requests.	By using the Software Portal, users can request and install software through a Web-based interface with little or no administrator involvement. See "About the Software Portal" on page 96.

Implementing Software Management Solution on Mac computers

Before you use Software Management Solution to manage software on Mac computers, you must set it up and prepare it for use.

The prerequisites for implementing Software Management Solution are as follows:

- Symantec Management Platform and Software Management Solution must be installed on the Notification Server computer.
  For details, see the *IT Management Suite Planning for Implementation Guide* at http://www.symantec.com/docs/DOC5670.
- The Symantec Management Agent must be installed or upgraded on the computers that you plan to manage.
  Software Management Solution requires that target computers be managed. A managed computer is one on which the Symantec Management Agent is installed.
- You must install or upgrade the Symantec Management Agent on the Mac computers that you plan to manage.
  The Software Portal for Mac is installed automatically with the Software Management Plug-in.

Table 6-3 Process for implementing Software Management Solution

Step	Action	Description
Step 1	Install or upgrade the Software Management Solution plug-in on managed computers. In Symantec Management Console, enable the policy.	The Software Management Solution plug-in is required for you to deliver and manage software on client computers. Perform this step every time that you need to install the Software Management Solution plug-in on the client computers that do not have it. The unified **Software Management Solution Plug-in Install** policy lets you install the solution plug-in on all supported operating systems. You may have performed this step when you installed the Symantec Management Platform or when you added new computers to the network.
Step 2	Configure security privileges for Software Management Solution.	Administrators need the appropriate privileges to deliver and manage the software in your organization. You or another administrator may have already performed this step when you configured security for the Symantec Management Platform. For more information, see the topics about setting up security and Software Management Solution settings in the *Symantec Management Platform Help*.
Step 3	Configure default settings for Managed Software Delivery.	You can configure the settings that control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies.

About Software Management Solution settings for Mac computers

Software Management Solution settings control the behavior of the software-related policies and tasks. The default settings let administrators create policies and tasks without having to enter the details that they are not familiar with. Instead, a more experienced administrator can configure the default settings that apply to all the new policies and tasks that are created. When necessary, the administrator who runs the specific policies and tasks can change the settings.

Table 6-4 Sources of default settings for Software Management policies and tasks

Policy or task	Source of default settings
Managed Software Delivery	All new managed software delivery policies inherit the default settings that are defined on the **Managed Delivery Settings** page. You can override the default settings for specific Managed Software Delivery policies. Changing the default settings for managed software delivery does not affect the execution of the managed software delivery policies that were created earlier.
Package Delivery Quick Delivery	Some of the task settings are predefined. Other settings for these tasks are obtained from the Task Management settings.

Installing Mac profiles using Software Management Solution

Software Management Solution lets you install and distribute the Mac profiles that consist of configuration including applications and the settings that you want to install on the Mac client computers.

To create Mac profiles using the Apple's Profile Manager, refer to the following URL:

About Profile Manager

After you create the Mac profile, you must create a software resource from the Mac profile file and then import the software package. After you create the software package, Software Management Solution lets you distribute the software package to the Mac client computers that are present in the network.

To distribute and install Mac profiles

1. Create a Mac profile that you want to distribute to Mac client computers.

   To create a Mac profile using the Apple's Profile Manager, refer to the following URL:

   About Profile Manager

2. In the Symantec Management Console, navigate to **Manage > Software Catalog** and click on **Import**.
3. Select **Software type** as **Software Release**.
4. Select the **Package source** as **Software Library**.

5 Click **Add** and select the profile file from the software resource that you have created. Click **Next**.

6 In the **Add or Edit Command Line** dialog box, add the **Command line** as `profiles -I -F ./<name of profile file>`

7 Click **OK**.

8 In the Symantec Management Console, navigate to **Actions > Software > Manage Software Delivery wizard** and create a **Quick Delivery Task** to distribute the Mac profile package to the Mac client computers.

For more information refer to the following URL:

http://www.symantec.com/docs/HOWTO84872

About software policy remediation on Mac computers

Managed Software Delivery lets you not only deliver software but also manage it. These actions ensure that you deliver the correct software to the correct computers.

When you schedule a Managed Software Delivery policy, you can assign different schedules for compliance and remediation. For example, you can schedule the compliance process to occur during the day and the remediation to occur only during a maintenance window.

Table 6-5 Compliance and remediation actions

Action	Description
Compliance	Compliance on Mac computers depends on the delivery method you select to install the software, as follows:Using Quick Delivery or Managed Delivery installs the software. ■ If you select Quick Delivery to install the software, then no detection is executed. In this case, you execute a command line command. To determine which software is installed on a Mac client computer, you must create a Software Inventory task that runs periodically and detects installed software. As a result of running this task, the information appears in Notification Server. ■ If you select Managed Software Delivery, when you execute delivery you first verify in your local cache if the software was installed previously. This cache is located inside the `swc.dat` file in the SMFagent on the client side. If a record of the software is present in that file, then delivery is not executed. If no information about the software is in the cache, then you execute a command line. You have the following options for ensuring that software appears in the cache: ■ If you installed the software manually, when you set Software Inventory to run the cache is also updated. ■ If software is installed using Managed Software Delivery, the cache is updated when the software delivery is executed.

Table 6-5 Compliance and remediation actions *(continued)*

Action	Description
Remediation	Remediation is the act of fixing any software that is out of compliance on the client computer. The nature of the remediation depends on the command-line action that the Managed Software Delivery policy performs. For example, an installation command runs when the compliance check returns False, and an uninstall command runs when the compliance check returns True. The following example illustrates how the installation command line determines the remediation action: Assume that you want to install antivirus software on all managed computers that do not have it installed. You create the Managed Software Delivery policy and select an installation command line. When the policy runs, the compliance check determines whether the specified antivirus software is installed.

About the Software Portal

The Software Portal lets users submit requests and install software through a Web-based interface with little or no administrator involvement. This self-service approach to software delivery reduces help desk calls and simplifies the process of requesting and delivering software. Because the Software Portal uses predefined software information and delivery settings, it can automate most of the deliveries that result from the software requests.

The administrator who sets up the Software Catalog decides which software each user or group of users is allowed and specifies which software requires approval. These settings determine the amount of intervention that is required for specific software requests. Requests for pre-approved software require no further action from anyone. Requests for other standard software require approval from a manager or an administrator but upon approval, the software delivery is automatic. Only the requests for non-standard software require the manager or the administrator to take further action to deliver the software.

The Software Portal is installed on the client computers. Therefore, the users can create requests and the managers can approve the requests without requiring access to the Symantec Management Console.

The Software Portal supports requests for Windows and Mac OS software.

Methods for delivering software to Mac computers

You can deliver software to one or more managed computers by creating and running a Software Management task or policy. The method that you use to create the task or policy depends on your delivery requirements.

Table 6-6 Methods for delivering software

Your requirement	Delivery method	Description
Deliver software to a specific computer or to a group of computers.	Drag and drop	In Symantec Management Console under **Manage > Software**, you can click and drag Deliverable software to a target. The target can be a single computer or a group of computers that you have already defined under **Manage > Computers** In the **Manage > Software** window, the **Installed Software** subpane lists the deliverable software packages that are on the server, including software releases and software updates. Deliverable software is the software that has a package or command line associated with it. If you drag and drop the package onto a computer, the package or command line installs the software. If software appears in this list, then it is ready to deploy. When you double-click a deliverable software package, the installation details open and you can define or make changes to the installation details.
Perform a Quick Delivery of a single software resource.	Quick Delivery	You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Quick Delivery uses the default task settings, which you can change when necessary. Because of its simplicity, Quick Delivery is an ideal way for non-administrators, such as help desk personnel, to deliver software safely and accurately. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog.

Table 6-6 Methods for delivering software *(continued)*

Your requirement	Delivery method	Description
Perform one or more of the following advanced delivery actions: ■ Deliver on a recurring schedule. ■ Install software with the other software that it depends on. ■ Install a software resource that replaces other software. ■ Sequentially install multiple software and tasks. ■ Run any client task at any stage of the delivery. A client task is one that is defined in Notification Server and is intended to run on a client computer.	Managed Software Delivery	Managed Software Delivery is a policy-based delivery method that lets you fulfill advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. Managed Software Delivery leverages the software resource information and the logic that is in the Software Catalog. For example, Managed Software Delivery uses the software resource's dependencies, package, and detection rule.
Deliver software in response to a direct request from a user.	Software Portal	With the Software Portal, users can request software and responds to those requests. If the user is pre-approved to install the software, the installation occurs without the administrator's involvement. Otherwise, the administrator only needs to approve the requests and deliver the software that is not in the Software Catalog. See "About the Software Portal" on page 96.
Deliver software with a policy that you migrated from Software Delivery Solution 6.x.	Legacy Software Delivery	When you upgrade from Notification Server 6.x to Symantec Management Platform 7.x, you can migrate your 6.x software delivery tasks to Legacy Delivery policies. You can continue to use those policies as they are. You can also assign their packages to software resources to deliver a 6.x software package with Quick Delivery or Managed Software Delivery.

Advanced delivery actions that Managed Software Delivery can perform with Mac computers

Managed Software Delivery is a policy-based delivery method that lets you respond to an assortment of advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions.

Table 6-7 Advanced delivery actions that Managed Software Delivery can perform

Delivery action	Description
Deliver software	In its simplest form, Managed Software Delivery delivers a single software resource with its associated package and command line. It downloads the software and installs it on the managed computer according to a defined schedule. It does not perform a compliance check and it always considers the computer to be compliant.
Remediate software on the client computer	Managed Software Delivery installs the software to a specific known state on the client computer. If the state of the software is out of compliance, Managed Software Delivery performs a remediation to restore the correct state.
Deliver software dependencies to the client computer as needed	Managed Software Delivery checks the client computer for the dependencies of a software resource that it delivers. When a client computer does not contain the dependency software, Managed Software Delivery can perform a remediation by installing the missing dependency. You can choose whether to check dependency tasks or not, with the following results: ■ If you do not choose to check dependency tasks, the Managed Software Delivery policy proceeds and either installs or fails. ■ If you choose to check dependency tasks, those tasks are checked and installed if necessary.
Sequentially install multiple software resources and tasks	You can deliver multiple software resources and tasks with a single Managed Software Delivery policy. You can add any client tasks to the execution queue to perform custom operations before, during, or after the software remediation process. For example, you can add a task that performs a restart or runs a script. A client task is one that is defined in Notification Server and is intended to run on a client computer.
Execute software installations offline	In a Managed Software Delivery policy, you can set different schedules for the compliance check and the remediation (in this case, installation). The separate schedules allow for the offline execution of the Managed Software Delivery. When the compliance check determines that a remediation is required, the policy downloads the appropriate package. Remediation can occur even if the client computer is not connected to the server because the client computer already has the package that it needs.

Creating a Managed Software Delivery policy with the Managed Software Delivery wizard for Mac computers

You can perform one or more advanced software delivery actions with a single Managed Software Delivery policy. Creating a Managed Software Delivery policy is the first step in performing an advanced software delivery.

The **Managed Software Delivery** wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. We recommend that you use the wizard because it can include any dependency software and warn you of software associations.

When you create a Managed Software Delivery policy with the **Managed Software Delivery** wizard, the policy is enabled automatically. If you do not want the policy to be available to managed computers immediately, edit the policy, and disable it. You can also edit the policy to add information about what to deliver.

The software that you deliver in this way must be defined as a software resource in the Software Catalog.

You can run the **Managed Software Delivery** wizard from the **Manage > Software** view or from other areas of the Symantec Management Console. Your point of entry into the **Managed Software Delivery** wizard determines the amount of default information that is populated.

Create the policy without the wizard if you need to do any of the following things:

- Add multiple software resources and tasks.
- Override the default settings.

To create a Managed Software Delivery policy with the Managed Software Delivery wizard

1. In the Symantec Management Console, on the **Manage** menu, click **Software**.
2. In the left pane, under **Deliverable Software**, click **Software Releases**.
3. Right-click a software resource and then click **Actions > Managed Software Delivery**.

   If the **Managed Software Delivery** option is not available, the software resource does not have a package associated with it and cannot be delivered. Click **Actions > Edit Software Resource** and configure the software resource.
4. In the **Managed Software Delivery** wizard, on the **Select software** page, specify the software to deliver and other delivery options and then click **Next**.
5. On the **Select destinations** page, specify the destinations to deliver the software to and then click **Next**.

6 On the **Schedule delivery** page, define the schedule for running the Managed Software Delivery and then click **Next**.

7 (Optional) On the **Specify dependencies and updates** page, select any dependencies, updates, or service packs that are defined for this software resource and then click **Next**.

Dependencies	Check **Verify dependencies** and select the check box for each dependency to include.
Updates or service packs	Select the check box for each update or each service pack to include.

8 To complete the wizard, click **Deliver Software**.

About using tasks to manage Mac computers

Apple has provided a large number of command line utilities that facilitate the management of Mac client computers. Many of these utilities have been used to create "run script" tasks in Symantec Management Console to let you run common tasks. The "run script" tasks that are available in the console let you take advantage of the built-in task server function in Symantec Management Platform. You deliver tasks to Mac computers by running these scripts.

See “About managing Macs with CMS” on page 12.

You may want to use tasks to deliver software and to configure security; for example, to lock down a client OS. You may also want to create tasks that you can deploy for power management or to wake up and power down managed Mac computers.

To configure Mac computers using tasks, you must write scripts to execute the tasks. If this skill is unfamiliar to you, please refer to the introduction to shell scripting that is available in the Mac OS X Developer Library. Symantec has also created a set of sample scripts that you can refer to as models for creating your own scripts. These are located in the Symantec Knowledge Base, HOWTO51884. The Symantec sample scripts are based on recommendations in these Apple Security Configuration guides.

Mac tasks fall into the following broad categories:

- Software delivery
- Security
- Power management.
  You can add the following tasks in the **Create New Task** window in the console under Power Control: Restart, Shut down, Log off, and Wake up

- Wake and power down

Configuring a software delivery task for Mac computers

You can deliver enterprise-class software to Mac computers using tasks that you run by creating a script.

You must follow the instructions that are found in the user guide of the software that you plan to deploy. If the software requires specific files and installers to support a silent installation, you must create them.

Ensure that you install the necessary files and installer to the correct directories. Use the exact installation path that the source media requires.

The process for configuring a software delivery task may vary depending on the software product that you install. The process that is laid out in the table illustrates how to install the *Adobe® Creative Suite® 4* software product. Each step links to a task that is part of this process. Because you may or may not choose to install this particular product, each task is presented as a sample.

Table 6-8 Process for configuring a software delivery task

Step	Description	Notes
Step 1	Complete software delivery prerequisites. Follow the instructions that are found in the *Adobe® Creative Suite® 4 Enterprise Manual Deployment User Guide* to create the necessary files and installer that support a silent installation. You can download the PDF can be downloaded from the Adobe site.	If you follow the instructions you produce the following required files for a silent installation: ■ application.override.xml ■ install.xml ■ remove.xml Make sure to save these files in the correct directories. The Adobe Installer appears to be hard-coded to search for certain payload items in the default path. For example, if the installer path is /Volumes/Adobe/CS4/payloads/…. but the installer looks in /Volumes/Adobe Creative Suite 4 Design Premium Disc 1/Adobe CS4 Design Premium/payloads/…. , you receive an error. When you create files or installers for the software that you want to deliver, use the exact path that the source media uses.
Step 2	Create a DMG file.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating a DMG file to deliver software to Mac OS X computers" on page 104.
Step 3	Create an Installer Shell script.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating an Installer Shell script to deliver software to Mac OS X computers" on page 105.

Table 6-8 Process for configuring a software delivery task *(continued)*

Step	Description	Notes
Step 4	If the software has its own installer, import the installer into the Software Catalog.	Read through or complete a sample task and then click the link to view the next step in the process. See "Importing an installer into the Software Catalog to deliver software to Mac OS X computers" on page 105.
Step 5	If the software includes a pop-up blocker, you can create a task to disable it.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating a task to disable the Product Improvement pop-up" on page 107.
Step 6	Update the Managed Software Delivery policy.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating a Managed Software Delivery policy to deliver software to Mac OS X computers" on page 108.

Creating a DMG file to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to create a DMG file for installing the *Adobe® Creative Suite® 4* software product.

See "About supported package-delivery formats for software distribution" on page 14.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task for Mac computers" on page 102.

To create a DMG file

1. On the Mac computer, in the Finder, navigate to the folder that contains the application file.
2. Right-click the folder, and select **Get Info**.

3 Record the size of the contents.

4 In Symantec Management Console, click **Applications > Utilities > Disk Utility**.

5 Click the **New Image** icon to create a new disk image.

6 Enter a name for the image. Select an adequate size or the size of the *Adobe® Creative Suite® 4* folder.

7 Set encryption to **None** and set **Format** to **read/write disk image**.

8 Place the contents of the *Adobe® Creative Suite® 4* folder into the newly mounted disk image.

9 Unmount the disk image.

Creating an Installer Shell script to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to create an Installer Shell script for installing the *Adobe® Creative Suite® 4* software product.

This task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task for Mac computers" on page 102.

To create an Installer Shell script

1 At the Mac Terminal, create a new shell script file and add the following line:

***setup.app path*/Contents/MacOS/Setup --mode=silent --deploymentFile=<install.xml or remove.xml path in quotes>**

Refer to the following sample:

```
/Volumes/Adobe/CS4/Setup.app/Contents/MacOS/Setup --mode=silent
--deploymentFile="/Volumes/Adobe/CS4/install.xml
```

2 Place this file and the DMG file that you created previously into a folder.

Warning: Do not include the shell script file in the DMG. You cannot select it as the installation file if it is inside the DMG.

Importing an installer into the Software Catalog to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to import the installer for the *Adobe® Creative Suite® 4* software product into the Software Catalog.

Copy the folder structure that you created previously to the Notification Server computer file share or to another Windows file share. The Software Library has a file size limit of 2GB and cannot accommodate the typically large file size of an *Adobe® Creative Suite® 4* installer.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task for Mac computers" on page 102.

To import the Adobe® Creative Suite® 4 installer into the Software Catalog

1. In Symantec Management Console, click **Manage > Software Catalog**.
2. In the **Software Catalog** window, under **Deliverable Software**, click **Import** to view a model dialog box.
3. Set **Software type** to **Software Release**.
4. Set the **Package source** to match the specific type of source on which your software is hosted.

   To install the software that is referred to in this sample task, you use Access package for a directory on Notification Server.
5. Browse to the installer location and select the folder that holds the DMG and shell script files.
6. Click **Display Location** to ensure that you have selected the correct folder.

   You should see your DMG and shell script files.
7. Click your shell script file (.sh) and then click **Set Installation File**.

   Caution: If you fail to set the installation file in this step, you cannot create command lines later.

   ---
8. Click **Next**.
9. Click **Create a new software resource**.
10. Give this software a meaningful name (for this sample task, a meaningful name is Adobe Creative Suite 4 Design Premium.
11. Set **Company** to Adobe Systems
12. Set **Version** to 4 or other specific version of the software that you choose to install.

13 Leave **Open software resource for editing when finished** selected.

Note: If you have a pop-up blocker enabled, disable it. A pop-up blocker prevents a new window from opening. if the window is blocked, locate the software in the list, highlight it, and click **Edit** (the pencil icon).

14 On the **Properties** tab, **Software Product** may be blank.

You can create a new Software Product named **Creative Suite**.

15 Click the **Package** tab.

A package was already created. However, a command line may not be there.

16 Click **Add command**.

17 In **Name** enter **Install**.

Description is optional.

18 Leave **Command line requires a package** selected.

The Adobe CS4 package should be selected by default.

19 In the **Package** field, your Adobe CS4 package should be selected by default.

20 Set the Installation file type to <other>.

21 Set the Command type to Install.

22 Click **Set** as the default for this command type.

23 Click **Edit** for the Command line.

24 Click the .**sh** file and then click **OK**.

The resulting command line should be *NameOfYourFile*.sh

25 Set the following **Success Codes**: 0, 8 (comma delimited)

26 Set **Failure Codes** to 1, 2, 6, 7, 9, 10, 11, 12, 13, 14.

These codes are specific to Adobe® Creative Suite® 4. Refer to the product PDF for details if you install this software product. If you follow the instructions in this sample task to install a different software product, refer to the product information for the failure codes.

27 Click **OK** and close the window.

Creating a task to disable the Product Improvement pop-up

(Sample)

This sample task illustrates how to disable the Adobe Product Improvement pop-up. This task runs after the *Adobe® Creative Suite® 4* software installation to disable the pop-up for new users.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task for Mac computers" on page 102.

To create a task to disable the Product Improvement pop-up

1. In Symantec Management Console, navigate to **Manage > Jobs and Tasks**
2. At the root of this folder, create a folder to work in.
3. Right-click the new folder and click **New > Task**.
4. Click **Run Script** to select that task type.
5. Give the task a descriptive name.

   You can use any descriptive name such as **Disable Adobe Product Improvement Program**.
6. Set the script type to UNIX Script.
7. Add the following string to the body:

   ```
   defaults write /Library/Preferences/com.adobe.headlights.APIP
   Enabled -int 0
   ```
8. Click **OK** to save the task.

Creating a Managed Software Delivery policy to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to create a Managed Software Delivery policy for installing the Adobe® Creative Suite® 4 software product.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task for Mac computers" on page 102.

To create a Managed Software Delivery policy

1. In Symantec Management Console, click **Manage > Policies**.
2. Click **Policies > Software > Managed Software Delivery**.
3. Right-click the **Managed Software Delivery** folder and click **New > Managed Software Delivery**.
4. Click the **New Managed Software Delivery** title and enter a descriptive name, or add an entry in the **Description** field.

5 Under **Policy Rules/Settings**, on the **Software** tab, click **Add > Software Resource**.

6 Select the software resource that you created previously, and click **OK**.

7 In the right pane, ensure that **Install Command** line and the correct CS4 software package are selected.

8 Click **Add > Task**.

9 Navigate to the **DisableAdobeProductImprovementProgram** task that you created earlier, highlight it, and click OK.

The task type is **Run Script**.

10 In the distribution tree, ensure that the task appears after the software.

11 On the **Policy Settings** tab, enter a meaningful display name.

You can include a description if you want to.

12 (Optional) On the **Software Publishing** tab, make this software available for users through the Software Portal.

13 On the far right in the **Policy Rules/Actions** area, click the Up arrow to collapse the section.

14 In the **Applied to** area, click **Apply to > Computers** to select the computers to which you want to apply this policy.

15 Beginning with all resources, click **Add rule** to filter out the computers to which you do not want to apply this policy.

16 Click **Add rule** again and continue to refine the results.

Refine the results until you are confident that you have applied this policy to the Mac computers for which you intend the policy.

As you refine the results, click **Update results** to list the resources that this policy targets.

Continue to filter the resource target so that it contains the exact subset of Mac computers to which you want the policy to apply.

17 Click **OK**.

18 Click the Up arrow on the right to collapse this area.

19 Click **Add schedule** to select a time to install the software.

Leave the **Remediation** option set to **Immediately**.

20 Save changes.

21 To turn on the policy click the red circle next to the **Off** label, click **On**, and click **Save**.

The software installs silently at the selected installation time.

Chapter 7

Using Patch Management Solution for Mac

This chapter includes the following topics:

- About Patch Management Solution for Mac
- Implementing Patch Management Solution for Mac
- About how Mac patching works
- About hosting an internal SUS to obtain internal software updates
- About patching Mac software
- Checking for available software updates
- Viewing the list of available software updates
- Redirecting a Mac client computer to a local SUS
- About the Mac compliance Dashboard
- Viewing reports
- Patch management for Mac return codes

About Patch Management Solution for Mac

Patch Management Solution for Mac lets you scan Mac computers for the updates that they require. The solution then reports on the findings and lets you automate the downloading and distribution of needed software updates. You can distribute all or some of the updates.

Patch Management Solution for Mac can update only the software that the Mac OS X software update utility supports. The solution integrates with the software update utility, and lets you collect needed update information from the target Mac computers and initiate a software update. Mac computers download software updates from the Apple website or from a Software Update Server (SUS) and report installation status information to Notification Server.

Patch Management Solution for Mac provides the preconfigured rollout jobs that let you automate installing a large number of updates. For example, the preconfigured rollout jobs can install all updates, all recommended updates, and so on.

See "Implementing Patch Management Solution for Mac" on page 112.

Implementing Patch Management Solution for Mac

The recommended workflow for updating Mac computers is as follows:

See "About Patch Management Solution for Mac" on page 111.

Table 7-1 Process for implementing Patch Management Solution for Mac

Step	Action	Description
Step 1	Install or upgrade the solution.	Use Symantec Installation Manager to install the solution.
Step 2	Install or upgrade the Symantec Management Agent.	Install or upgrade the Symantec Management Agent for UNIX, Linux, and Mac on the target Mac computers. See "About installing the Symantec Management Agent for UNIX, Linux, or Mac" on page 21.

Table 7-2 Process for installing software updates

Step	Action	Description
Step 1	Check for available updates.	You can check target Mac computers for the software updates that they require. See "Checking for available software updates" on page 114.
Step 2	Install all or some of the updates.	You can install individual updates or use batch rollout jobs.
Step 3	View installation status reports.	Use reports to view the software update compliance and rollout job status. See "Viewing reports" on page 119.

About how Mac patching works

All Mac computers need to have direct Internet access. All Mac computers download updates from Apple.com.

Without allowing Mac client computers Internet access, the only way you can still patch Mac software is to use a Software Update Server (SUS). In this case, you must redirect all clients to the SUS on the Mac OS X server.

Software Update Server is part of the OS X Server operating system and contains a repository of all available updates. The OS X Server must be connected to the Internet to download Apple updates. Mac clients can then be redirected to the SUS service on the OS X Server.

The Software Update utility is built in to each client Mac. Users can run the `softwareupdate` command from time to time or on a schedule like a Windows scheduled task.

If a Mac client has Internet access, then the user can update software. The software update utility runs on the Mac client and presents available services or updates. The user selects the desired services or updates, which are then downloaded through the GUI on the client.

About hosting an internal SUS to obtain internal software updates

You can allow Mac client computers direct access to the Apple software update site or host a Software Update Server (SUS) internally.

See "Redirecting a Mac client computer to a local SUS" on page 116.

Symantec recommends that you allow direct client access to the Apple software download site rather than setting up a SUS.

Hosting a SUS is a task for advanced Mac administrators because setup is somewhat complex. Setup requires that you change settings manually on every Mac client. To simplify the process, you can create an image, install it on all Mac computers, and then run scripts to change the settings.

The benefit to hosting a SUS internally is that you download software updates from Apple one time and then distribute software updates over the network. This method is more secure and requires lower bandwidth than having Mac clients download software directly over the Internet.

Note that a SUS is not part of Symantec Management Platform or CMS; however, you can host it on the same network. See Management scripts, including setting liveupdate server (SUS) and Mac SUS server setup.

About patching Mac software

Patching software to keep it up to date is a common administrator task. In the Mac world, you run a software update utility.

See "About managing Macs with CMS" on page 12.

To keep software on Mac computers up to date, you run a scheduled client task on each Mac. This task invokes the local software update utility, `softwareupdate -l` (the letter ell stands for the word local). This utility finds the software that is available for installation. When you run the `softwareupdate -l` command, you see a list of applicable updates.

The software update utility passes results back to Notification Server for central reporting, and the results are stored in the Configuration Management Database (CMDB).

You can update the software in the following ways:

- Use Task Server to selectively schedule the installation of one or many software updates.
  Some updates require a restart. When you schedule updates with Task Server, you can allow end-user notifications so that users are aware that updates need to be installed.
  In Symantec Management Console, under the **Reports** menu, you can get a list of which computers require a restart.
- Run pre-built jobs out of box to enable automatic patching.

Checking for available software updates

You can check target Mac computers for the software updates that they require. When you run the **Check Available Updates Task**, the target Mac computers download software update information from Apple and then report the list of available updates to Notification Server.

To ensure that the list of available software updates on Notification Server is kept up-to-date, schedule the task to run twice a week. Configure the task to run on the **All Patchable Mac Computers** target.

If you want to quickly check Mac computers for compliance, you can run the task immediately.

After you collect software update information from Mac computers, you can view this information in reports.

See "Viewing the list of available software updates" on page 115.

See "Implementing Patch Management Solution for Mac" on page 112.

To check for available software updates

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **System Jobs and Tasks > Software > Patch Management > Mac**, and then click **Check Available Updates Task**.
3. Under **Task Status**, click **New Schedule**.
4. Under **Schedule**, do one of the following:
   - If you want to run the task immediately, click **Now**.
   - If you want to schedule the task, click **Schedule**, and then configure the schedule. Symantec recommends that you schedule this task to run twice a week.
5. Under **Input**, click **Add > Target**.
6. Click **Open**.
7. In the **Open** dialog box, click **All Patchable Mac Computer Target**, and then click **OK**.
8. Click **OK**.
9. Click **Schedule**.

Viewing the list of available software updates

You can view the list of available software updates in the **Available Mac Software Updates for computers managed by this server** report. The report also shows the number of computers that require an update.

In reports, you can drill down on specific items to obtain additional information.

To populate the report, collect the available software updates inventory.

See "Checking for available software updates" on page 114.

See "Implementing Patch Management Solution for Mac" on page 112.

To view the list of available software updates

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Software > Patch Management > Mac**, and then click **Available Mac Software Updates for computers managed by this server**.

Redirecting a Mac client computer to a local SUS

Symantec recommends that you allow direct client access to the Apple software download site. An alternative is to set up a Software Update Server (SUS), which is complex and requires substantial manual configuration.

Although it is not recommended that you configure a local Software Update Server (SUS) to manage Apple software updates, it can be done. After you configure the SUS, the Altiris Patch Management for Mac 7.1 from Symantec solution then pulls the software updates locally. This method can be more efficient and require fewer network resources than allowing every Mac client to pull updates individually from the Apple Web site .

See "About hosting an internal SUS to obtain internal software updates" on page 113.

If you decide to redirect a Mac client to a local SUS, the option you choose depends on which user or users should be affected. It also depends on which tool should be affected, such as GUI or command line utility.

Note: The port specification is required only if your update server uses a port other than the default port or ports.

You can direct client back to Apple rather than the local Software Update Server. To redirect a client, you remove the preference setting that points to an internal server. In this case, you have two options. You can delete the modified setting and allow the client computer to revert to Apple for software updates. Another option is to remove the preference settings altogether by deleting the files from both the user's home folders and the root home folder.

Redirecting a Mac client computer to a local SUS

1. On the Mac client computer, click **Finder > Applications > Utilities > Terminal.app** to open a Terminal window (command prompt).
2. Update the preference setting for the user or group by executing the relevant command:

The local user who is running the command updates own preference setting. This method only affects the GUI Software Update tool.	`defaults write com.apple.SoftwareUpdate CatalogURL "http://update.server.address:8088/"`
You (the administrator) update the global settings for all users on a system. This method only affects the GUI Software Update tool.	`defaults write /Library/Preferences/com.apple.SoftwareUpdate CatalogURL "http://update.server.address:8088/"`
The root user (a local user using `sudo` to get administrator privileges) updates own global settings. This method affects the command-line softwareupdate utility.	`sudo defaults write com.apple.SoftwareUpdate CatalogURL "http://update.server.address:8088/"`

To remove the preference settings and allow the client computer to revert to Apple for software updates

1. On the Mac client computer, click **Finder > Applications > Utilities > Terminal.app** to open a Terminal window (command prompt).
2. Perform an appropriate `defaults read` action to validate the information to be deleted.

   You can execute the `defaults read` command to make sure that you do want to delete the information that you are about to delete.
3. Remove the settings using one of the following commands:

The local user who is running the command removes own settings.	`defaults delete com.apple.SoftwareUpdate CatalogURL`
You (the administrator) update the global settings for all users on a system.	`defaults delete /Library/Preferences/com.apple.SoftwareUpdate CatalogURL`
The root user.	`sudo defaults delete com.apple.SoftwareUpdate CatalogURL`

To remove the preference settings

1. On the Mac client computer, click **Finder > Applications > Utilities > Terminal.app** to open a Terminal window (command prompt).
2. Remove the software update configuration for the account in one of the following ways:

   If you set up the SUS from a user's account, then you should remove it from that account using the `rm ~/path` command. Adding the tilde (~) means "Go to this user's account." This command lets you delete the account for the current user.

The root account.	`rm /Library/Preferences/com.apple.SoftwareUpdate.plist`
Individual user account.	`rm ~/Library/Preferences/com.apple.SoftwareUpdate.plist`

About the Mac compliance Dashboard

This portal page provides patch management summary information at a glance. The page is comprised of a number of Web Parts displaying results from commonly used reports.

You can access the home page by clicking **Home > Patch Management**, and then, under **Mac OS X**, clicking **Compliance Dashboard**.

Table 7-3 Web Parts on the **Mac Software Update Compliance Portal** page

Report	Description
Getting Started	Displays the recommended Patch Management Solution for Mac implementation workflow.
Mac Software Update Compliance	Reports the number of Mac computers that require or do not require an update.
Mac Software Update Delivery Summary	Displays the list of software update rollout jobs and the number of computers that succeeded or failed to run the job.

Viewing reports

Patch Management Solution for Mac reports let you view the software update compliance and rollout job status.

See "Implementing Patch Management Solution for Mac" on page 112.

Table 7-4 Patch Management Solution for Mac reports

Report	Description
Mac Updates Not Installed by Computer	Displays information about updates available for installation on Mac computers managed by this server. To populate this report, you must run the **Check Available Updates Task**. See "Checking for available software updates" on page 114. You can create software update rollout jobs and install updates directly from this report.

Table 7-4 Patch Management Solution for Mac reports *(continued)*

Report	Description
Mac Software Update Compliance	Displays the percentage of computers that require an update. To populate this report, you must run the **Check Available Updates Task**. See "Checking for available software updates" on page 114.
Mac Software Update Installation Status	Displays the software update rollout job status. The number in the **Succeed** column indicates the number of times the job has run, regardless of whether the update was needed.
Mac System Assessment Scan Summary	Displays the list of last assessment scans for each Mac computer managed by this server.
Mac Computers - Updates Not Installed	Displays the number of updates not installed on each Mac computer, managed by this server.

To view Patch Management Solution for Mac reports

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Software > Patch Management > Mac**.
3. Click the report that you want to view.

Patch management for Mac return codes

When you run client tasks within the default rollout jobs that are created with Patch for Mac, you can expect to see certain return codes. If you need to do some troubleshooting, the information in the following quick-reference table can help you interpret what the codes mean. The table lists return values and their meanings. The information in the table was reproduced from a Symantec Connect blog post. View the Symantec Connect blog post here.

0	Installation finished successfully
1	Installation finished successfully Restart required

2	Update installation failure
3	Update installation failure Restart required
4, 127	Invalid command line options
5	`softwareupdate` utility failure
6	Error parsing output of `softwareupdate` utility
7	Error communicating with Symantec Management Agent

Chapter 8

Imaging and Deploying Mac computers

This chapter includes the following topics:

- About supporting Macintosh computers
- Prerequisites for Mac computer setup
- Launching Symantec's Mac pre-OS Creation Utility
- Configuring NBS for Mac computers
- Creating preboot configuration for Mac
- Adding or importing predefined computers
- Booting Mac computers with NetBoot image
- Installing Mac OS using Deployment Solution
- Creating and deploying Mac images

About supporting Macintosh computers

Deployment Solution supports Macintosh computers of an enterprise network to set up, execute, and report on the deployment-related tasks that are executed on the computers. Some of the deployment-related tasks of the Deployment Solution for Mac computers are imaging, installing operating system and so on. Similar to Windows and Linux computers, Mac computers too are driven by the Symantec Management Agent and the Deployment Solution plug-in for execution of any deployment-related tasks on the computers.

Deployment Solution supports set up of the Mac computers that can be categorized into unknown, predefined, or managed. A new Mac computer that is added in a network without a computer name or IP address and is unmanaged by the Symantec Management Platform (SMP) is called the unknown computer. A predefined Mac computer is a computer for which you add the details such as computer name, MAC address and so on to the Symantec Management Platform even before the computer is added to the network. You can add the computer name and the hardware identifier through the SMP console and the details are stored in the database. Managed computers are the ones on which the Symantec Management Agent is installed and are managed by the SMP.

The key features that are supported for the Mac computers are as follows:

- Booting Mac computers in preboot environment
- Imaging Mac computers
- Installing the Mac OS
- Performing system configuration after deploying an image.

Deployment Solution leverages these features even without the presence or connection with the Apple Server. Mac computers boot in the preboot environment using a NetBoot image or in an automation environment using an automation folder. An automation environment is installed on the client computer when the **Deployment Automation folder for Mac - Install** policy is enabled from the SMP. A NetInstall image is required for installing a Mac OS on the client computer. A NetBoot image and a NetInstall image can be created using the Symantec's Mac pre-OS Creation Utility (MOCU) of the Deployment Solution along with the Apple's System Image Utility. Deployment Solution also facilitates creation of jobs and tasks for Mac computers through the **Jobs and Tasks** page of the console. In the console you can access the **Jobs and Tasks** page by navigating to **Manage > Jobs and Tasks > Deployment and Migration**.

Deployment Solution lets you perform the following tasks on Mac computers:

- **Create Image**
- **Deploy Image**
- **Install Mac OS**
- **Apply System Configuration**
- **Boot To**

See "About Symantec's Mac pre-OS Creation Utility" on page 126.

See "Launching Symantec's Mac pre-OS Creation Utility" on page 125.

Prerequisites for Mac computer setup

Following are the prerequisites that you must comply with before you use Deployment Solution to manage you Macintosh (Mac) client computers:

- Ensure that you add the following services on the site server on which you enable the NBS service before you check **Enable Mac Netboot (BSDP) support** in the **NBS General Settings** dialog box :
  - Windows Role Services for Network File System (NFS) in File Services for Windows
  - Windows Services for UNIX (SFU) for UNIX
- Configure the DHCP server in the network. The Network Boot Server (NBS) and the DHCP server must be on different computers.
- Install the Symantec Management Agent and the Deployment Solution plug-in for Mac on the source volume and ensure that the Deployment Automation folder for Mac - Install policy is installed on the NetBoot image source computer. Symantec recommends that you install the Symantec Management Agent and the Deployment Plug-in for Mac clients as a root user.
  You can access the plug-ins through either of the following menus:
  - **Settings > Agent/Plug-ins > All Agent/Plug-ins**
    On the left pane of the window, access **Agent/Plug-ins > Deployment and Migration > Mac** folder.
  - **Settings > All Settings**
    On the left pane of the window, access **Agents/Plug-ins > Deployment and Migration > Mac** folder.
  - **Actions** > **Deployment** > **Install Deployment Plug-in** > **Mac**.
- Install the Apple's Server Admin Tool, that has an app named, System Image Utility on the Mac source computer. The installer version of the Apple's Server Admin Tool must be compatible with the booted Mac OS version.
- The Mac preboot image creator must be logged in as the root user of the source computer.
- Ensure that you have at least the same amount of empty space on the booted source volume as occupied by the installed Mac OS.
- Ensure that you set the following for the **All Linux/Mac Workstations** and the **All UNIX/Linux/Mac Servers** in the **Targeted Agent Settings** dialog box before adding a Mac client computer in the network:
  - **Return the following information as computer name** as DNS name

- **Return the following information as computer domain** as DNS name

You can access the **Targeted Agent Settings** from **Settings > Agents/Plug-ins**.

See "About Symantec's Mac pre-OS Creation Utility" on page 126.

See "Launching Symantec's Mac pre-OS Creation Utility" on page 125.

Launching Symantec's Mac pre-OS Creation Utility

The Symantec's Mac pre-OS Creation Utility of Deployment Solution lets you create and modify the Mac NetBoot image and the NetInstall image. The NetBoot image is used as a preboot image to boot client computers in preboot environment. The NetInstall image is a type of preboot image that is used along with the configuration file to install Mac operating system on client computers. After you create a NetBoot image or a NetInstall image ensure that you modify the image using the Mac pre-OS Creation Utility and upload the image to the Notification Server computer. The NetBoot image and the NetInstall image are then distributed from the Notification Server computer to all the site servers with Network Boot Service (NBS) installed. The NBS supports only .dmg images that are shared over the Network File System (NFS). The HTTP protocol is not supported for sharing images.

Before you use the Mac pre-OS Creation Utility ensure that you comply with the prerequisites for using Mac computers for deployment-related tasks.

See "Prerequisites for Mac computer setup " on page 124.

Note: Ensure that you do not access the `Automation` folder and the `Agent` folder that is placed in the `<install_dir>/Program Files/Altiris/Notification Server/NSCap/bin/UNIX/Deployment/Mac/universal/` path from a Mac client computer using the Server Message Block (SMB) shares.

To launch Symantec's Mac pre-OS Creation Utility

1. On the Notification Server computer, navigate to the `<install_dir>/Program Files/Altiris/Notification Server/NSCap/bin/UNIX/Deployment/Mac/universal/MocuAppInstaller` path and download the MOCUInstaller.pkg uitlity on the source computer.
2. Install the MOCUInstaller.pkg on the volume of the source computer, which is installed with the Symantec Management Agent, the Deployment plug-in for Mac, and the policies.

   You use the utility to create and modify the NetBoot image and the NetInstall image.
3. To launch the application on your Mac source computer, navigate through **Finder > Go > Applications** and double-click on the MOCU.app.

See "Creating and modifying NetBoot images " on page 127.

See "Creating and modifying NetInstall images" on page 129.

About Symantec's Mac pre-OS Creation Utility

The Symantec's Mac pre-OS Creation Utility of Deployment Solution lets you create and modify Mac NetBoot image and NetInstall images. This utility along with Apple's System Image Utility lets you create the Mac NetBoot image either from a booted volume or from a bootable volume of the source computer. Ensure that the booted volume or the bootable volume is installed with the Symantec Management Agent and the Deployment Solution plug-in for creating the NetBoot image. The NetInstall image is used to install Mac OS on the client computers.

A NetBoot image is used to boot Mac clients into diskless mode and is used in the **Create Image**, **Deploy Image**, and **Boot To** tasks. The modified NetBoot image that is prepared using the Mac pre-OS Creation Utility contains bootable OS files, Symantec Management Agent, and the Deployment Solution plug-in. The NetBoot image does not contain Mac OS files and therefore cannot be used for installing the Mac operating system. The NetBoot image is used to boot the client computers in the preboot environment

A NetInstall image is a type of preboot image that is used to install Mac operating system on the client computers. The NetInstall image contains the required Mac operating system files that are available in the Mac OS distribution media. In Deployment Solution, you use the **Install Mac OS** task to install Mac OS on client computers. The **Install Mac OS** task uses the modified NetInstall image and the configuration file to carry out the installation of Mac operating system without human assistance.

After you create a NetBoot image or a NetInstall image ensure that you modify the image using the Mac pre-OS Creation Utility and upload the image to the Notification Server computer. The NetBoot image and the NetInstall image are then distributed from the Notification Server computer to all the site servers with Network Boot Service (NBS) installed. The NBS supports only .dmg images that are shared over the Network File System (NFS). The HTTP protocol is not supported for sharing images.

See "Launching Symantec's Mac pre-OS Creation Utility" on page 125.

See "Creating and modifying NetBoot images " on page 127.

See "Creating and modifying NetInstall images" on page 129.

Creating and modifying NetBoot images

Deployment Solution lets you create and modify Mac NetBoot images using the Symantec's Mac pre-OS Creation Utility and the Apple's System Image Utility. These images are then used to boot Mac clients in preboot environment. Ensure that you modify the NetBoot image using the Mac pre-OS Creation Utility so that the image is compatible with Deployment Solution. Symantec recommends that the NetBoot source is booted with the combo update of the supported operating system.

After you modify the NetBoot image, you must upload the NetBoot image to the Notification Server computer. You can do this using the **Add Preboot Configuration** dialog box. The NetBoot image is then distributed to all the Network Boot Servers in the network.

See "Creating preboot configuration for Mac" on page 134.

Ensure that Symantec Management Agent, and Deployment Solution plug-in for Mac are installed on the NetBoot image source volume and the Deployment Automation folder for Mac- Install policy is installed on the source computer

If you face an error, it can be verified in the Console's application. To access the application go to **Finder > Utilities** and launch **console.app** application.

To view logs of Apple's System Image Utility, go to **Menu > View > Show Log**.

You can create and modify Mac NetBoot images from the following sources:

- Mac booted volume
  The Mac booted volume of the source computer is the current volume in which the client computer is booted.
- Mac bootable volume

The Mac bootable volume of the source computer is any volume other than the booted volume on which Mac operating system is installed and is used to create a NetBoot image.

To create and modify Mac NetBoot image from Mac booted volume

1. Launch the Symantec's Mac pre-OS Creation Utility.
2. In the Mac pre-OS Creation Utility, select **NetBoot** from **Create and Update image**.
3. Click **Next**.
4. Enter the **Temporary Volume Name**.

   You can estimate the size of the temporary volume by clicking the **Estimate Size**.
5. Click **Prepare Temporary Volume**.

   Ensure that you have emptied the **Trash** before creating the temporary volume.
6. Click **Next**.
7. Click **Launch System Image Utility**.
8. In the Apple's System Image Utility, enter the **Type**, **Installed Volume**, **Save To**, **Image name**, and **Description**. The **Network disk** and the **Image Index** must be left as default. A message is displayed if the NetBoot image (.nbi) is created successfully.
9. In the Symantec's Mac pre-OS Creation Utility, click **Choose...** from **Select image to update**. To modify a NetBoot image select the NetBoot.dmg.
10. Click **Update Image** to modify the image (.dmg file) and make it suitable to be used for Deployment Solution tasks.

    Save the modified image on your computer and then upload it to the Notification Server computer.

To create and modify Mac NetBoot image from bootable volume

1. Launch the Mac pre-OS Creation Utility.
2. In the Mac pre-OS Creation Utility, select **NetBoot** from **Create and Update image**.
3. Click **Next**.
4. Click **Next** again.
5. Click **Launch System Image Utility**.

6 In the Apple's System Image Utility, enter the **Type**, **Installed Volume**, **Save To**, **Image name**, and **Description**. The **Network disk** and the **Image Index** must be left as default. A message is displayed if the NetBoot image (.nbi) is created successfully.

7 In the Symantec's Mac pre-OS Creation Utility, click **Choose...** from **Select image to update** and select the image (.dmg) to modify.

8 Click **Update Image** to modify the image (.dmg) and make it suitable to be used for Deployment Solution tasks.

Save the modified image and then upload it to the Notification Server computer.

See "About Symantec's Mac pre-OS Creation Utility" on page 126.

See "Launching Symantec's Mac pre-OS Creation Utility" on page 125.

Creating and modifying NetInstall images

A NetInstall image along with the Mac configuration file is used to install Mac OS on a client computer. The Symantec's Mac pre-OS Creation Utility and the Apple's System Image Utility lets you create and modify NetInstall image. You must modify a NetInstall image to make it compatible with Deployment Solution. If, you modify an existing NetInstall image, ensure that it is created using the latest version of Deployment Solution. After modifying the NetInstall image, you must upload the image to the Notification Server computer. From the Notification Server computer the image is then distributed to all the Network Boot Servers (NBS) present in the network.

If you check any any errors, you can check the following logs:

- System.log file
  To view Symantec's Mac pre-OS Creation Utility logs, view the log in the System.log file.
- Console.app
  To access the console application's logs, go to **Finder > Utilities** and open **Console.app**.
- Show log
  To view the Apple's system Image Utility logs, go to **Menu** > **View** > **Show Log** of the utility.

To create and modify NetInstall image

1 Launch the Symantec's Mac pre-OS Creation Utility.

2 In the Mac pre-OS Creation Utility, select **NetInstall** from **Create and Update Image**.

3 Click **Next**.

4 On the page that is displayed, click **Launch System Image Utility**. Save the NetInstall image on your computer.

Ensure that the **Enable Automated Installation** is included after the **Define Image Source** in the workflow while creating a NetInstall image using the Apple's System Image Utility.

5 In the Apple's System Image Utility, enter the **Type**, **Installed Volume**, **Save To**, **Image name**, and **Description**. The **Network disk and the Image Index** must be left as default.

6 In the Mac pre-OS Creation Utility, click **Choose...** from **Select image to update**. Browse and select the NetInstall.dmg image.

7 Click **Update Image**.

To modify NetInstall image

1 Launch the Symantec's Mac pre-OS Creation Utility application.

2 In the Mac pre-OS Creation Utility, select **NetInstall** from **Create and Update Image**.

3 Click **Next**.

4 On the page that is displayed, click **Choose...** from **Select image to update**. Browse and select the NetInstall.dmg image.

5 Click **Update Image**.

See "About Symantec's Mac pre-OS Creation Utility" on page 126.

See "Launching Symantec's Mac pre-OS Creation Utility" on page 125.

See "About Mac configuration file" on page 155.

Configuring NBS for Mac computers

The **NBS General Settings** option of the Network Boot Service (NBS) lets you configure one or more site servers with the preboot configuration settings. For Mac, the preboot configuration setting is used to configure the client computers to boot in the pre-OS or the preboot environment using a NetBoot image. The preboot configurations are applicable for the unknown computers, managed computers, and predefined computers of an enterprise network.

You can access the **NBS General Settings** option from the following menu of the console:

- **Settings > Notification Server > Site Server Settings**

In the **Site Management** view pane, access **Settings > Network Boot Service > Settings > NBS General Setting**

- **Settings > Deployment > NBS General Settings**

To configure the NBS settings

1 In the Symantec Management Platform (SMP) console, click **Settings > Deployment > NBS General Settings**.

2 In the **NBS General Settings** dialog box, configure the following **Network Boot Service Configuration** settings:

Network Boot Service Configuration	Lets you configure the Network Boot Service (NBS) for a site server. To enable or disable the policy, you must select the **Turn On** or **Turn Off** icons on the right side of the dialog box or page.
Apply NBS settings immediately	Check the option if you want to apply the NBS policy immediately on the site servers. If the option remains unchecked then the NBS configurations changes are applied as scheduled in the Symantec Management Agent (SMA) for rolling out policies.
Enable the NBS service	Check the NBS service to enable the service on the site server. By default, this option is checked.
Enable Mac Netboot (BSDP) support	Check the Netboot (BSDP) support to enable Mac client computers to boot using the Mac NetBoot images. Ensure that you add the following services on the site server on which you enable the NBS service before you check **Enable Mac Netboot (BSDP) support**: ■ Windows Role Services for Network File System (NFS) for Windows ■ Windows Services for UNIX (SFU) for UNIX
Reset button	Lets you restore the previous configuration that you performed for the NBS site server.

3 In the **NBS General Settings** dialog box, for the **Initial Deployment (Unknown Computer) Menu** configure the following settings:

Netboot menu (Mac) tab — Set these options to repond to the unknown computers that are added in the network.

- **Respond to unknown computers**
  Check this option if you want to respond to the unknown computers to configure them to NetBoot environment.
- **Default Boot image**
  Select the default NetBoot image with which you want to boot the client computers.

4 In the **NBS General Settings** dialog box, for the **Redeployment (Predefined Computer) Menu** configure the following settings:

Netboot menu (Mac) tab — Set these options to repond to predefined computers added in the network.

- **Respond to Predefined computers**
  Check this option if you want to respond to the predefined computers to configure them to NetBoot environment.
- **Default Boot image**
  Select the default NetBoot image with which you want to boot the client computers.

5 In the **NBS General Settings** dialog box. for the **Redeployment (Managed Computer) Menu** configure the following settings:

Netboot menu (Mac) tab — Set these options to respond to the managed computers.

- **Respond to Managed computers**
  Check this option if you want to respond to the managed computers to configure them to NetBoot environment.
- **Default Boot image**
  Select the default NetBoot image with which you want to boot the client computers.

6 Click **Save changes**.

7 Again, in the console, click the **Settings > Deployment > NBS Global Settings** menu.

8 In the **NBS Global Settings** dialog box or pane, click **Save Changes**.

See “About NBS General Settings ” on page 133.

About NBS General Settings

The **NBS General Settings** option of the Network Boot Service (NBS) lets you configure one or more site servers with preboot configuration settings. The preboot configuration settings are required to configure the client computers to boot in the pre-OS or preboot environment using a PXE image or NetBoot image. A PXE image is related to the Windows or Linux preboot environments whereas a NetBoot image is related to the Mac environment. Computers of UEFI architecture can boot in the preboot environment using the x64-bit PXE image of Windows. Deployment Solution categorizes preboot configuration settings for unknown computers, managed computers, and predefined computers.

The **NBS General Settings** configuration is applicable only when NBS is installed on the site server and the service is enabled.

See “Installing Network Boot Service on site server” on page 133.

You can access the **NBS General Settings** option from the following menus of the console:

- **Settings > Notification Server >Site Server Settings**
  In the **Site Management** view pane, access **Settings > Network Boot Service > Settings > NBS General Setting**.
- **Settings > Deployment > NBS General Settings**

Installing Network Boot Service on site server

Network Boot Service (NBS) is a component of Deployment Solution that you install and run as a service on a site server. This service is independent of the presence of Task service or Package service on a site server and handles all communication with the Symantec Management Platform (SMP) for Deployment Solution. You must install the Microsoft XML Core Services 6.0 on the site server on which you install the NBS component. The NBS comprises of the PXE and BSDP service and the TFTP service that are installed on the site server after you roll out the NBS service through the SMP console.

After the NBS is installed, the status of the service is displayed as green and the service status is displayed as **Started**.

You must install and enable the Network Boot Service (NBS) service on the site server before you create preboot configuration and start configuration of NBS settings.

Note: If you want to install the Deployment Package server component and the NBS on the same site server, then you must install the Deployment Package Server component after installing the NBS on the site server.

To install NBS service on site server

1. In the Symantec Management Console, navigate to **Settings > Notification Server > Site Server settings** menu.
2. In the **Site Management** window, expand **Site Server** node in the tree.
3. On the **Site Servers** page, click **New** under the **Detailed Information** pane.
4. In the **Select Computers** dialog box, select the Windows computers that you want to configure as site server and click **OK**.
5. In the **Add/Remove services** dialog box, check the **Network Boot Service** option for the site servers that you select.

Creating preboot configuration for Mac

Deployment Solution lets you create Mac preboot environments. The preboot configuration is required to boot client computers in the preboot environment or the pre-OS state. Deployment Solution lets you create two types of preboot environments for Mac operating system such as NetBoot environment and NetInstall environment.

For Mac, you create NetBoot environment using the images that are created before creating the preboot environment. The NetBoot environment is used to boot the client computer in preboot environment. You can also create a NetInstall environment to boot client computers in the preboot environment and install Mac OS without manual intervention using the Mac configuration file.

See "Creating and modifying NetBoot images " on page 127.

To use the preboot configuration, you must have the administrative rights and the User Account Control (UAC) settings disabled.

You can access either of the following menus to create and configure a preboot environment:

- **Settings > Deployment > Create Preboot Configuration**
- **Settings > All Settings > Deployment & Migration > Create Preboot Configuration**

To create a preboot configuration

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Create Preboot Configurations**.
2. In the **Create Preboot Configurations** dialog box, click **Add**.
3. In the **Add Preboot Configurations** dialog box, enter the name and description of the preboot configuration.

Operating system	Select Mac operating system.
OEMextention	Select DS Agent as the OEM agent .
Select Mac Preboot Environment to upload	These options are available when you select Mac as the operating system. You can select either of the following: ■ **NetBoot** You can create a NetBoot configuration environment by selecting NetBoot. ■ **NetInstall** You can create a NetInstall configuration environment by selecting NetInstall. Browse and select the NetBoot or NetInstall folder (<name>.nbi) by clicking on the folder icon. To select a folder that is placed on a UNC location use, \\<ipaddress>\<shared folder> in the **File Name**.

4. On the **Add Preboot Configurations** page, click **OK**.
5. On the **Preboot Configurations** page, click **Save changes**.

See "Configuring NBS for Mac computers" on page 130.

Adding or importing predefined computers

Deployment Solution lets you provision client computers even before they are added to the network as predefined computers. You add the predefined computer details or import them from a .txt file or a .csv file. Both addition and import of predefined computer details can be performed through the Symantec Management Platform (SMP) console.

To add a predefined computer

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Predefined Computers**.
2. In the **Predefined Computer** dialog box, click **Add**.
3. In the **Add Predefined Computer Settings** page, specify the values for the fields that are as follows:

Name	Lets you specify a name for the predefined computer. This field is mandatory.
Serial Number	Lets you specify the serial number of the computer. The value of this hardware identifier is used by Deployment Solution as a matching criteria to identify unknown client computers of a network as potential predefined computers.
Asset Tag	Lets you specify the asset tag of the computer.
UUID	Lets you specify the Universal Unique Identifier (UUID) of the computer. The value of this hardware identifier is used by Deployment Solution as a matching criteria to identify unknown client computers of a network as potential predefined computers.
Host Name	Lets you specify the host name of the computer.
Domain/Workgroup	Lets you specify the domain of the computer.

Network Adapters

Lets you select the type of network adapter that you want to add as predefined computer. Click **Add** if you want to add more than one adapters.

The options to select from are as follows:

- **Use DHCP to obtain IP address**
  By default, this option is selected.
  Select this option if you want to select the IPaddress of computers using DHCP. Specify the values for the required fields that appear after you select this option.
  The fields that you can specify are as follows:
  - MAC Address
    The value of this hardware identifier is used by Deployment Solution as a matching criteria to identify unknown client computers of a network as potential predefined computers.
  - DNS 1, DNS2, DNS3
  - Primary DNS Suffix
  - Primary WINS Server
  - Secondary WINS Server
- **Assign static IP address**
  Select this option if you want to specify a static IP address of the computers. Specify the values for the required fields that appear after you select this option.
  The fields that you can specify are as follows:
  - MAC Address
    The value of this hardware identifier is used by Deployment Solution as a matching criteria to identify unknown client computers of a network as potential predefined computers.
  - IP Address
  - Default Gateway
  - Subnet Mask
  - DNS 1, DNS2, DNS3
  - Primary DNS Suffix
  - Primary WINS Server
  - Secondary WINS Server

Note: The MAC address is mandatory for the Mac client computers.

4 Click **OK**.

To import predefined computer

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Predefined Computers**.
2. In the **Predefined Computer** dialog box, click **Import Computers**.
3. In the **Open File** dialog box, navigate to the `.txt` or the `.csv` file that contains the information about the computers to import.

   You can copy a sample `Pre-DefinedComputers.csv` file from the `\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\Sample\PreDefinedComputers` folder.
4. From the **Manage** menu, select **Computers** to view the details of imported predefined computers.

Booting Mac computers with NetBoot image

Deployment Solution lets you boot different types of Mac computers such as unknown or bare metal computers, predefined computers, or managed computers in the preboot environment or the automation environment using a NetBoot image. A NetBoot image is created using the Apple's System Image Utility and must be modified before you use it in Deployment Solution. You can create and modify a NetBoot image using the Symantec's Mac pre-OS Creation Utility.

See "Launching Symantec's Mac pre-OS Creation Utility" on page 125.

To boot a Mac computer, besides the NetBoot image, you also require to configure the site server on which the Network Boot Service (NBS) is installed.

The NBS settings let you configure the default response setting for unknown, predefined, and managed Mac computers. The default response of the Mac client computer is set based on the NetBoot image that you configure for the type of client computer. The client computer then boots in the preboot environment using the NetBoot image. You must hold the N key of the keyboard while booting the Mac computer that is added into the network to receive the default NetBoot image.

The basic steps that you must execute to prepare the environment for booting Mac computers with NetBoot images are as follows:

Table 8-1 Booting Mac clients in preboot environment

Step	Action	Description
Step 1	Launch the console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install the Network Boot Service on a site server	Install the Network Boot Service on the site server. See "Installing Network Boot Service on site server" on page 133.
Step 3	Create and modify a NetBoot image	Create and Modify a NetBoot image using the Symantec's Mac-preOS Creation Utility. See "Creating and modifying NetBoot images " on page 127.
Step 4	Create preboot environment	Create the preboot environment with the NetBoot image.
Step 5	Enable the NBS service to support Boot Service Discovery Protocol (BSDP)	Enable the BSDP support from the NBS general settings. See "Configuring NBS for Mac computers" on page 130.

Table 8-1 Booting Mac clients in preboot environment *(continued)*

Step	Action	Description
Step 6	Configure response for unknown, predefined, and managed computers	From the NBS General Settings page, set response for unknown, predefined, and managed Mac computers. You can boot the following types of Mac clients: ■ Unknown Mac clients See "Booting an unknown Mac computer in NetBoot environment" on page 143. ■ Predefined Mac clients See "Booting a predefined Mac computer in NetBoot environment" on page 146. ■ Managed Mac clients See "Booting a managed Mac computer in NetBoot environment" on page 149.

See "Booting an unknown Mac computer in NetBoot environment" on page 143.

See "Booting a predefined Mac computer in NetBoot environment" on page 146.

See "Booting a managed Mac computer in NetBoot environment" on page 149.

Creating a Boot To task

You can start computers in an automation environment to run tasks, else boot to a PXE environment or a production environment based on the requirement.

You can use either PXE environment or automation environment but not both environments together. Assign this task only if you want to perform a custom automation task.

To create a Boot to task

1. In the Symantec Management Console, select **Manage > Jobs and Tasks**.
2. In the left pane, do either of the following:
   - Right-click **System Jobs and Tasks** folder and select **New > Task**.
   - Expand the **System Jobs and Tasks** folder and right-click **Deployment and Migration** folder to select **New > Task**.

3 In the **Create New Task** dialog box, under **Deployment and Migration** folder, select the **Boot to** task.

4 The fields and the descriptions are as follows:

Task name icon	Displays the default task name as Boot To. You can edit the default task name to specify a relevant task name. For example, Boot To_Automation.
Automation	Lets you select the automation environment to boot the client computers. Automation environment is created on the client computers on which the automation folder is installed.
Production	Lets you select the production environment to the boot the computer either from the preboot environment or automation environment. You boot a computer into the production environment to resume regular tasks such as report generation or so.

PXE/Netboot

Lets you select the PXE image for the WinPE or LinuxPE environments or the NetBoot image for the Mac environment from the drop-down list.

For the PXE image, select any of the following architectures from the drop-down list:

- **Auto**
  Select this option if you want to boot the client computer based on the computer's processor architecture. For example, if you have a client computer whose processor type is x64 but the installed operating system is x86 of Windows 7, then the **Auto** option boots the computer in x64 architecture mode and not in x86 mode.
  The **Auto** option can be useful if you have created a common PXE image for both x86 and x64 architectures or want to boot a computer as per the processor architecture irrespective of the OS architecture. You create PXE images through the **Create Preboot Configuration** dialog box of the console.
- **x86**
  Select this option if the PXE image that you have created is for the x86 architecture of the operating system.
- **x64**
  Select this option if the PXE image that you have created is for the x64 architecture of the operating system.

Note: Before you boot to PXE, ensure that you have started the Windows firewall service and opened the ports 4011 and 69. Otherwise, booting to PXE might fail.

Registration Period	The registration time period is the time period during which the client computers are unrolled from Notification Server registration policy. This happens only when the client computer tries to boot from one environment to another. Within the specified registration time, the client computer must again register back to the registration policy, failing which, the computer must be registered manually. The default registration time that is displayed is the registration time that is set in the **Global Settings** page.

5 Click **OK**.

6 Schedule the task.

Booting an unknown Mac computer in NetBoot environment

Deployment Solution lets you boot an unknown Mac computer in the preboot environment using a NetBoot image. An unknown client computer is not managed by the Symantec Management Platform (SMP).

To boot an unknown client computer with the default NetBoot image, hold the N key of the keyboard while booting the Mac computer that is added in the network.

The following process elaborates the steps that are involved to boot a client computer in NetBoot environment using a NetBoot image when an unknown computer is added in the network:

Table 8-2 Process for booting an unknown Mac computer with NetBoot image

Step	Action	Description
Step 1	Launch the Console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install the Network Boot Service on a site server	Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See "Installing Network Boot Service on site server" on page 133.
Step 3	Create and modify a NetBoot image using Symantec's Mac pre-OS Creation Utility	Create and modify a NetBoot image that is used to boot the Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. This utility along with Apple's System Image Utility is used to create and modify the NetBoot image to make it compatible for Deployment Solution. See "Creating and modifying NetBoot images " on page 127.

Table 8-2 Process for booting an unknown Mac computer with NetBoot image *(continued)*

Step	Action	Description
Step 4	Create preboot environment	Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer. It is then distributed to all the NBS in the network.
Step 5	Enable the NBS service to support Boot Service Discovery Protocol	Enable the following services in the **Network Boot Service Configuration** pane of the **NBS General Settings** dialog box: ■ **Enable the NBS service** ■ **Enable Mac NetBoot (BSDP) support** See "Configuring NBS for Mac computers" on page 130.
Step 6	Configure response for unknown computers	In the NBS General Settings, set default response for unknown computers. In the **Netboot menu (Mac)** of **Initial Deployment (Unknown Computer) Menu**, select the **Respond to unknown computers** and select the **Default Boot image** from the list of NetBoot images that are configured from the **Create Preboot Configuration** menu of the console. See "Configuring NBS for Mac computers" on page 130.

Table 8-2 Process for booting an unknown Mac computer with NetBoot image *(continued)*

Step	Action	Description
Step 7	Boot the client computer in preboot environment	Turn on your Mac client with the DHCP IP enabled and hold the N key of the keyboard. The client computer searches for the Network Boot Server (NBS) by broadcasting Boot Service Discovery Protocol (BSDP) requests. NBS receives and processes this BSDP request. The client then receives and boots the default NetBoot image as set in the NBS in step 6. On booting the unknown computer with the NetBoot image its inventory is added and displayed in SMP as a predefined computer.

See "Booting Mac computers with NetBoot image" on page 138.

Booting a predefined Mac computer in NetBoot environment

Deployment Solution supports Mac operating system and lets you boot predefined Mac client computer in preboot environment. A predefined computer is a computer whose details are added in the Symantec Management Platform. You add the predefined computer details or import them from a .txt file or a .csv file.

The following process elaborates the steps that are involved to boot a predefined Mac client computer in preboot environment using a NetBoot image:

Table 8-3 Process for booting a predefined Mac client in preboot environment with NetBoot image

Step	Action	Description
Step 1	Launch the console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install the Network Boot service on a site server	Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See "Installing Network Boot Service on site server" on page 133.
Step 3	Add or import a predefined computer	You can add predefined computers using the **Add Predefined Computers Settings** dialog box or import predefined computers using a .txt file or a .csv file. See "Adding or importing predefined computers" on page 135.

Table 8-3 Process for booting a predefined Mac client in preboot environment with NetBoot image *(continued)*

Step	Action	Description
Step 4	Create and modify a NetBoot image using Symantec's Mac pre-OS Creation Utility	Create and modify a NetBoot image to be installed on a Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. This utility along with the Apple's System Image Utility is used to create and modify the NetBoot image to make it compatible for Deployment Solution. See "Creating and modifying NetBoot images" on page 127.
Step 5	Create preboot environment	Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer from where it is distributed to all the NBS in the network.
Step 6	Enable the NBS service to support Boot Service Discovery Protocol	In the **Network Boot Service Configuration** of the **NBS General Settings** page enable the following services: ■ **Enable the NBS service** ■ **Enable Mac NetBoot (BSDP) support** See "Configuring NBS for Mac computers" on page 130.

Table 8-3 Process for booting a predefined Mac client in preboot environment with NetBoot image *(continued)*

Step	Action	Description
Step 7	Configure response for predefined computers in NBS	In the NBS General Settings, set the default response for the predefined computers. Configure the NBS to respond to the predefined Mac computers and set the default image. See "Configuring NBS for Mac computers" on page 130.
Step 8	Boot the client computer in preboot environment	Turn on your Mac client with DHCP IP enabled and hold the N key of the keyboard. The client computer searches for the Network Boot Server (NBS) by broadcasting BSDP requests. NBS receives and processes this BSDP request. The client receives and boots the default NetBoot image as set in the NBS in step 7.

See "Booting Mac computers with NetBoot image" on page 138.

Booting a managed Mac computer in NetBoot environment

Deployment Solution lets you boot a managed Mac client computer in preboot environment with NetBoot image. A managed computer is the one that is managed by the Symantec Management Platform.

You can boot a managed Mac client in the preboot environment using a NetBoot image or you can boot a Mac client in automation environment using the DSAutomation volume. The DSAutomation volume is installed on the Mac client computer by enabling the **Deployment Automation folder for Mac - Install** policy.

See "Setting up automation environment on Mac computers" on page 167.

The following process elaborates the steps that are involved in booting a managed Mac computer in preboot environment:

Table 8-4 Process for booting a managed Mac client in preboot environment

Step	Action	Description
Step 1	Launch the Console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install the Network Boot Service on a site server	Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See "Installing Network Boot Service on site server" on page 133.
Step 3	Create and modify a NetBoot image using Symantec's Mac pre-OS Creation Utility	Create and modify NetBoot image that is used to boot the Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. This utility along with Apple's System Image Utility is used to create and modify the NetBoot image to make it compatible for Deployment Solution. See "Creating and modifying NetBoot images " on page 127.

Table 8-4 Process for booting a managed Mac client in preboot environment *(continued)*

Step	Action	Description
Step 4	Create preboot environment	Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer from where it is distributed to all the NBS in the network.
Step 5	Enable the NBS service to support Boot Service Discovery Protocol	Enable the following services in the **Network Boot Service Configuration** from the **NBS General Settings** dialog box. ■ **Enable the NBS service** ■ **Enable Mac NetBoot (BSDP) support** See "About NBS General Settings " on page 133.
Step 6	Configure response for managed computers in NBS or Create a **Boot To** task.	You can do either of the following: ■ In the NBS General Settings set default response for managed computers. Configure NBS to respond to managed Mac computers and set the default image. See "Configuring NBS for Mac computers" on page 130. ■ You can also boot a managed Mac computer using the **Boot To** task. See "Creating a Boot To task" on page 140.

Table 8-4 Process for booting a managed Mac client in preboot environment *(continued)*

Step	Action	Description
Step 7	Boot the client computer in preboot environment	Turn on your Mac client and hold the N key. The client computer searches for the NBS by broadcasting BSDP requests. NBS receives and processes this BSDP request. The client then receives and boots the default NetBoot image as set in the NBS in step 6. If you have scheduled a **Boot To** task, the client computer receives the task as scheduled. See "Creating a Boot To task" on page 140.

See "Booting Mac computers with NetBoot image" on page 138.

Installing Mac OS using Deployment Solution

Deployment Solution lets you install Mac operating system on client computers. You can perform OS installation using the **Install Mac OS** task.

You can access the **Install Mac OS** task from the console's **Manage > Jobs and Tasks > Create New Task > Install Mac OS**.

You can execute Mac OS installation for the following:

- Unknown computers
  See "Installing Mac OS on an unknown computer" on page 156.
- Predefined computers
  See "Installing Mac OS on a predefined Mac computer" on page 159.
- Managed computers in automation or NetBoot environment
  See "Installing Mac OS on a managed computer" on page 163.

Ensure that the client computer hard drive has proper partitions and the target volume is correctly mentioned in the configuration file before you perform the **Install Mac OS** task on the client computers

You can access the Mac configuration file from the following location:

`<instaldir>\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\Deployment\Mac\NetInstall\AnswerFile\`

After performing the operating system installation, if the client computer is not able to connect to Symantec Management Platform, then you must manually install the Symantec Management Agent

To view the logs, go to

`<instal_Volume>/var/tmp/AltirisAgentInstallStartup/` and click `AltirisAgentInstallStartupLog.txt`.

If you want to install Mac OS on multiple client computers, you must do the following settings to ensure that correct inventory details are displayed on the Notification Server computer

- Go to **Settings > Agents/Plug-ins > Targeted Agent Settings > All Linux/Mac Workstations**. In the **UNIX/Linux/Mac** tab, set the following in the **Computer information**:
  Return the following information as computer name as **DNS name**.
  Return the following information as computer domain as **DNS name**.
- Go to **Settings > Agents/Plug-ins > Targeted Agent Settings > All UNIX/Linux/Mac Servers**. In the **UNIX/Linux/Mac** tab, set the following in the **Computer information**:
  Return the following information as computer name as **DNS name**.
  Return the following information as computer domain as **DNS name**.

To perform Mac OS installation

1. In the Symantec Management Console, from **Manage** menu select **Jobs and tasks**.
2. Right-click **Jobs and tasks** and select **New Task**.
3. On the **Create new task** page, select **Install Mac OS**.

4 In the **Install Mac OS** task page, you must specify the values for the fields.

The fields and descriptions are as follows:

Task name icon	Lets you specify the Install Mac OS task name.
OS Flavor	Lets you select the OS version for Mac from the drop-down list.
OS NetInstall Image	Lets you select the NetInstall image. Ensure that you have modified the NetInstall image using the Symantec's Mac pre-OS Creation Utility and uploaded the image to Notification Server computer. You can upload the NetInstall image by creating a preboot configuration for the NetInstall image. See "Creating and modifying NetInstall images" on page 129.
Configuration File	Lets you browse for the configuration file that you want to use for the installation. The configuration file stores answers for the required parameters during installation of the operating system. The configuration file is placed at <instaldir>\NSCap\bin \UNIX\Deployment\Mac\NetInstall\AnswerFile\ **Note:** Symantec recommends that you set the ShouldErase parameter as `False`. If you set it as `True`, then you must select the drive, on which the Mac operating system must be installed and install the Symantec Management Agent and Deployment Plug-in manually on the client computer. See "About Mac configuration file" on page 155.

5 Click **OK**.

See "Installing Mac OS on an unknown computer" on page 156.

See "Installing Mac OS on a predefined Mac computer" on page 159.

See “Installing Mac OS on a managed computer” on page 163.

About Mac configuration file

In Deployment Solution, a configuration file is also known as the answer file and stores parameters for an operating system (OS) installation. You can customize a configuration file to perform an unattended OS installation.

The configuration file for Mac operating system is in the following location of the computer on which SMP is installed:

```
<instaldir>\Program Files\Altiris\Notification
Server\NSCap\bin\UNIX\Deployment\Mac\NetInstall\AnswerFile\
```

Refer to Apple's support documentation to know more about the parameters.

http://www.apple.com/support/

Note: For mass installation of Mac operating system, do not specify the `TargetUUID` parameter. The `TargetUUID` parameter is unique for every client computer and interrupts mass operating system installation.

Following are the parameters that you can customize in a Mac configuration file:

Table 8-5 Parameters for Mac configuration file

Parameter	Description
InstallType	You can set the type of installation as automated. You can set the type of installation as automated if the workflow in the Apple's System Image Utility includes Enable Automated Installation while creating the NetInstall image
Language	You can set the preferred language of operation.
Package	Set the Package name with the folder location. By default it is set as >/System/Installation/Packages/OSInstall.mpkg

Table 8-5 Parameters for Mac configuration file *(continued)*

Parameter	Description
ShouldErase	Symantec recommends setting the `ShouldErase` parameter as `False`. If you set it as `True`, then you must select the drive, on which the Mac operating system must be installed and install the Symantec Management Agent and Deployment Plug-in manually on the client computer.
Target	Set the target volume where the operating system has to be installed. By default it is set to `Volumes/Macintosh HD`.

See "Installing Mac OS using Deployment Solution" on page 152.

Installing Mac OS on an unknown computer

Deployment Solution lets you install Mac operating system on an unknown Mac computer. An unknown computer is not managed by the Symantec Management Platform (SMP). For Mac computers, you must first boot the computer in preboot environment and then install the Mac operating system.

Following process elaborates the steps that are involved in installing Mac operating system on an unknown Mac computer:

Table 8-6 Process for installing Mac operating system on unknown Mac client

Step	Action	Description
Step 1	Launch the Console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console

Table 8-6 Process for installing Mac operating system on unknown Mac client *(continued)*

Step	Action	Description
Step 2	Install the Network Boot service on a Site Server	Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See "Installing Network Boot Service on site server" on page 133.
Step 3	Create and modify NetBoot image and NetInstall image using Symantec's Mac pre-OS Creation Utility	Create and modify NetBoot and NetInstall image to be installed on Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. See "Creating and modifying NetBoot images " on page 127. See "Creating and modifying NetInstall images" on page 129.
Step 4	Create preboot environment	Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server from where it is distributed to all the NBS in the network.

Table 8-6 Process for installing Mac operating system on unknown Mac client *(continued)*

Step	Action	Description
Step 5	Enable the NBS service to support Boot Service Discovery Protocol and configure response for unknown computer in NBS	Enable **Enable the NBS service** and **Enable Mac NetBoot (BSDP) support** in Network Boot Service Configuration from the **NBS General Settings** dialog box In the **NBS General Settings** page, configure NBS to respond to unknown Mac computers and set the default image. **Note:** Ensure that the NetBoot image is modified using the Symantec's Mac pre-OS Creation Utility to make it suitable for Deployment Solution. See "Configuring NBS for Mac computers" on page 130.
Step 6	Boot the client computer in preboot environment	Turn on your Mac client and hold the N key. The client computer searches for the NBS by broadcasting BSDP requests. NBS receives and processes this BSDP request and the client receives and boots the default NetBoot image as set in the NBS in step 5.

Table 8-6 Process for installing Mac operating system on unknown Mac client *(continued)*

Step	Action	Description
Step 7	Create an **Install Mac OS** task and schedule it for the client computer	Create an **Install Mac OS** task to install the Mac operating system. Specify the details of the target volume in the configuration file on which you want to install the operating system. If you want to clean the disk and partition it, do it before running the task. You must manually erase and partition the disk for Mac computers. To run the task immediately, use the **Quick Run** option. You can also schedule the task for the client computer. See "Installing Mac OS using Deployment Solution" on page 152.

See "Installing Mac OS using Deployment Solution" on page 152.

Installing Mac OS on a predefined Mac computer

Deployment Solution lets you add predefined computers to a network and also install a Mac operating system on them. You can either add the details of predefined computers using the **Add Predefined Computers Settings** or import them using a .txt file or a .csv file. For Mac predefined computers, you must specify the MAC address of the computer. You must first boot the Mac predefined computer in the preboot environment and then install the Mac operating system on the client computer.

The following process elaborates the steps that are involved to install the Mac operating system on a predefined Mac computer using a NetInstall image:

Table 8-7 Process for installing Mac operating system on a predefined Mac computer

Step	Action	Description
Step 1	Launch console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Install the Network Boot service on a site server	Install the Network Boot Service (NBS) on a site server before you perform any other configurations. See "Installing Network Boot Service on site server" on page 133.
Step 3	Add or import a predefined computer	You can add predefined computers using the **Add Predefined Computers Settings** dialog box or import predefined computers using a .txt file or a .csv file. See "Adding or importing predefined computers" on page 135.

Table 8-7 Process for installing Mac operating system on a predefined Mac computer *(continued)*

Step	Action	Description
Step 4	Create and modify NetBoot image and NetInstall image using Symantec's Mac pre-OS Creation Utility	Create and modify the NetBoot and NetInstall images before you install the Mac OS on a Mac client computer. Create and modify the NetBoot image and the NetInstall image to be installed on a Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. This utility along with the Apple's System Image Utility is used to create and modify the NetBoot image and the NetInstall image to make them compatible for deployment-related tasks See "Creating and modifying NetBoot images" on page 127. See "Creating and modifying NetInstall images" on page 129.
Step 5	Create preboot environment.	Create a preboot environment with the NetBoot image. The preboot environment ensures that the NetBoot image is uploaded on the Notification Server computer from where it is distributed to all the NBS in the network.

Table 8-7 Process for installing Mac operating system on a predefined Mac computer *(continued)*

Step	Action	Description
Step 6	Enable the NBS service to support Boot Service Discovery Protocol and configure response for predefined computers	Turn on the **Enable the NBS service** and **Enable Mac NetBoot (BSDP) support** in **Network Boot Service Configuration** from the **NBS General Settings** page. In the **NBS General Settings** page, set the default response for the predefined computers. Configure the NBS to respond to the predefined Mac computers and set the default image. See "Configuring NBS for Mac computers" on page 130.
Step 7	Boot the client computer in preboot environment	Turn on your Mac client and hold the N key. The client computer searches for the NBS by broadcasting BSDP requests. NBS receives and processes this BSDP request and the client receives and boots the default NetBoot image as set in the NBS in step 6.

Table 8-7 Process for installing Mac operating system on a predefined Mac computer *(continued)*

Step	Action	Description
Step 8	Create an Install Mac OS task and schedule it for the client computer.	Create an **Install Mac OS** task to install the Mac operating system. Specify the details of the target volume in the configuration file on which you want to install the new operating system. If you want to clean the disk and partition it, do it before running the task. You must manually erase and partition the disk for Mac computers. To schedule, you can either use the **Quick Run** option or schedule the task for the client computer. See "Installing Mac OS using Deployment Solution" on page 152.

See "Installing Mac OS using Deployment Solution" on page 152.

Installing Mac OS on a managed computer

Deployment solution lets you install the Mac operating system on a managed computer. A managed computer is managed by the Symantec Management Platform (SMP) and is installed with the Symantec Management Agent (SMA). Deployment Solution lets you install the Mac operating system on a specific volume of the managed client computer.

Following process elaborates the steps that are involved in installing the Mac operating system on a managed Mac computer:

Table 8-8 Process for installing Mac operating system on a managed Mac client

Step	Action	Description
Step 1	Launch the Console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Create and modify the NetInstall image using Symantec's Mac pre-OS Creation Utility	Create and modify NetInstall image to be installed on Mac client computer. You can do this using the Symantec's Mac pre-OS Creation Utility. See "Creating and modifying NetInstall images" on page 129.
Step 3	Create preboot environment.	Create a preboot environment with the NetInstall image. The preboot environment ensures that the NetInstall image is uploaded on the Notification Server from where it is distributed to all the NBS in the network.
Step 4	Enable the NBS service to support Boot Service Discovery Protocol	Enable the **Enable the NBS service** and **Enable Mac NetBoot (BSDP) support** in Network Boot Service Configuration pane of the **NBS General Settings** dialog box. See "Configuring NBS for Mac computers" on page 130.

Table 8-8 Process for installing Mac operating system on a managed Mac client *(continued)*

Step	Action	Description
Step 5	Create and schedule an Install Mac OS task	Create an **Install Mac OS** task, to install the Mac operating system. Specify the details of the target volume in the configuration file on which you want to install the new operating system. If you want to clean the disk and create new partitions, do it before running the task, you must manually erase the disk and create new partitions on the disk for Mac computers To schedule, you can either use the **Quick Run** option or schedule the task for the client computer. See "Installing Mac OS using Deployment Solution" on page 152.

See "Installing Mac OS using Deployment Solution" on page 152.

Creating and deploying Mac images

Deployment Solution lets you create and deploy Mac images. Imaging of a client computer involves copying the applications and settings of a computer into an image which is then deployed on other computers.

To create Mac images use the **Create Image** task and to deploy an image use the **Deploy Image** task in any preboot mode of the client. The client computer can be booted in preboot environment using a NetBoot image or in the automation environment using the `DSAutomation` volume. You can access the **Create Image** task and the **Deploy Image** task from the **Manage > Jobs and Tasks** menu.

Note: Mac imaging is not supported on HTTP or HTTPS. You must have the **Publish UNC codebase** check box checked in the **Package Server Settings** page.

The following process elaborates the steps that are involved in creating and deploying Mac images on client computer:

Table 8-9 Creating and deploying Mac image

Step	Action	Description
Step 1	Launch the console	Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://<IP address of NS>/altiris/console
Step 2	Boot the image source client computer to preboot environment	You must boot the image source client computer to preboot environment using one of the following: ■ NetBoot image ■ Automation folder See "Booting Mac computers with NetBoot image" on page 138.
Step 3	Create image of the source Mac computer	You use the **Create Image** task to create an image of the source computer after you boot the computer in the preboot environment or automation environment See "Creating a Mac image" on page 168.

Table 8-9 Creating and deploying Mac image *(continued)*

Step	Action	Description
Step 4	Boot the target client computer to preboot environment	You must boot the target client computer to preboot environment on which you want to deploy the image using one of the following: ■ NetBoot image ■ Automation folder See "Booting Mac computers with NetBoot image" on page 138.
Step 5	Deploy image on the target computer	Deploy the image on Mac computers using the **Deploy Image** task. See "Deploying a Mac image" on page 170.

Setting up automation environment on Mac computers

An automation environment for a Mac client computer is a setup that is created on the client computer by installing a Mac automation folder. The automation folder or an automation volume lets you boot the client computer in an automation environment. The automation volume is installed on a Mac client computer using the **Deployment Automation folder for Mac - Install** policy.

The **Deployment Automation folder for Mac - Install** policy creates a `DSAutomation` volume on the disk volume where Symantec Management Agent (SMA) is installed. The automation volume uses only the available space on the volume that is installed with SMA and does not use any free space available on other volumes. Ensure that there is sufficient space on the volume on which you have installed the SMA. The approximate size of the automation folder that is created on the client computer is 15 GB. If, a volume is already present with the name, `DSAutomation` then a new volume of name `DSAutomationA` is created.

You can also uninstall the automation volume with the uninstall policy for Mac automation folder. After you enable the **Deployment Automation folder for Mac - Uninstall** policy you must manually delete the DSAutomation partition that is present in the unmounted and unallocated state. If you do not want to run the uninstall policy to uninstall the automation folder from the client computer, then you must manually erase the disk and the volume from the client computer. If, you

manually erase the disk and the volume of the client computer, then ensure that you clean the Non-volatile random-access memory (NVRAM) of the client computer.

To clean the NVRAM of a client computer, refer to http://support.apple.com/kb/HT1533 article.

You can access the policy through either of the following:

- **Settings > Agents/Plug-ins**
  On the left pane of the window, access **All Agents/ Plug-ins > Deployment and Migration > Mac** folder.
- **Settings > All Settings**
  On the left pane of the window, access **Agents/ Plug-ins > Deployment and Migration > Mac** folder.

To install an automation folder

1. In the Symantec Management Console, on the **Settings** menu, click **Agent/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, expand the **Agents/Plug-ins > Deployment and Migration** folders.
3. Choose Mac installation and expand the corresponding folder.
4. Click the **Automation Folder - Install** policy.
5. In the right pane, in the **Program name** box, ensure that the correct policy is selected.
6. Under **Applied to**, select the client computers that you want to install the plug-in on.
7. Under **Schedule**, select when you want to install the plug-in.
8. (Optional) Click **Advanced** to check if the computers you selected are available at the exact time that you scheduled.

   You can also select start and end dates on this page.
9. Under **Extra schedule options**, select the options that you want.
10. Ensure that the policy is enabled.

    A green **On** symbol shows in the top right corner.
11. Click **Save changes**.

Creating a Mac image

Deployment Solution lets you create the Mac images that you can use to deploy on client computers. You can use predefined tokens to image Mac client computers.

Before you create a Mac image ensure to comply with the following:

- The Mac image source computer is booted in preboot or automation environment.
- The Mac image source client computer has its IP configured as dynamic and receives it from the DHCP server in the network.

To create a Mac image

1. In the Symantec Management Console, select **Manage > Jobs and Tasks**.
2. In the left pane, do either of the following:
   - Right-click **System Jobs and Tasks** folder and select **New > Task**.
   - Expand the **System Jobs and Tasks** folder and right-click **Deployment and Migration** folder to select **New > Task**.
3. In the **Create New Task** dialog box, under the **Deployment and Migration** folder select the **Create Image** task.
4. In the **Create Image** dialog box, specify the details for the following:

Task name icon	Displays the default task name as **Create Image**. You can edit the default task name to specify a relevant task name. For example, Create Image_Mac10.7.
Image Name	Enter the name of the image that you want to create.
Description	Enter the details of the image that you want to create.
Imaging tool	Select the imaging tool as **symDeploMac** to image the Mac computer.

5. In the **Create Image** task pane, click the **Advanced...** button.
6. In the **Advanced** dialog box, in the **Command line** tab, set the **Source disk (-SRC)**.

   You must enter the details of the disk name and the partition or the volume number of the image source of the Mac client computer. The format to enter the **Source disk (-SRC)** is `diskname:partition or volume number`.

   For example 1:2, here 1 is the disk name and 2 is the partition number or volume number of the Mac client computer. To know the Mac disk name and partition details of the Mac client computer, navigate to **Go > Utilities > Terminal** and enter the command `diskutil list`.

On executing the command, the details of the Mac client computer are displayed. For example, disk0s1, disk0s2, disk2s1 and so on. Here for disk0s1, disk0 is the disk name and 1 is the partition number or the volume number.

In Deployment Solution, the **Source disk (-SRC)** field starts with 1, here 1 corresponds to the disk 0 of the Mac computer. Similarly 2 corresponds to disk 1 of the Mac computers and so on.

Following are few examples of the disk name and partition number format that should be entered in the **Source disk (-SRC)** field:

- For disk0s2 specify the value as 1:2, where 1 is the disk name and 2 is the partition number.
- For disk1s2 specify the value as 2:2, where 1 is the disk name and 2 is the partition number.
- For disk2s1 specify the value as 3:1, where 3 is the disk name and 1 is the partition number.
- For disk2s2 specify the value as 3:2, where 3 is the disk name and 2 is the partition number.

See "Creating and deploying Mac images" on page 165.

See "Deploying a Mac image" on page 170.

Deploying a Mac image

Deployment Solution lets you deploy Mac disk images on one or more Mac computers. The Mac disk image is hardware-dependent and cannot be deployed across different models of computers of the same make.

For Mac client computers, following settings must be done to ensure that correct inventory details are displayed on the Notification Server computer:

- In the Symantec Management Console, go to **Settings > Agents/Plug-ins > Targeted Agent Settings.**
  In the left pane of the **Targeted Agent Settings** page, select **All Linux/Mac Workstations** option.
  In the **All Linux/Mac Workstations** page, select the **UNIX/Linux/Mac** tab and set the following in the **Computer information**:
  - **Return the following information as computer name** as **DNS name**
  - **Return the following information as computer domain** as **DNS name**.
- In the Symantec Management Console, go to **Settings > Agents/Plug-ins > Targeted Agent Settings.**

In the left pane of the **Targeted Agent Settings** page, select **All Linux/Mac Servers** option.

In the **All Linux/Mac Servers** page, select the **UNIX/Linux/Mac** tab and set the following in the **Computer information**:

- **Return the following information as computer name** as **DNS name**
- **Return the following information as computer domain** as **DNS name**.

To deploy a Mac image

1. In the Symantec Management Console, select **Manage > Jobs and Tasks**.
2. In the left pane, do either of the following:
   - Right-click **System Jobs and Tasks** folder and select **New > Task**.
   - Expand the **System Jobs and Tasks** folder and right-click **Deployment and Migration** folder to select **New > Task**.
3. In the **Create New Task** dialog box, under the **Deployment and Migration** folder select the **Deploy Image** task.

   In the **Deploy Image** task pane, specify the following details:

Task name icon	Displays the default task name as **Deploy Image**. You can edit the default task name to specify a relevant task name. For example, Deploy Image_Mac10.7.
Imaging	Select or browse the Mac image with `a.mac` extension that is to be deployed on the client computer.

Deploy Image Options

Lets you enter the details about deploying the image on the client computer.

Click the **Advanced** button.

In the **Advanced** dialog box, enter details for the following:

- **Partition**
  In the **Partition** tab, select the **Resize partition proportionately** to resize disk partitions.

  Note: If there is empty disk space present on the computer then it is merged with the last partition of the Mac computer.

- **Command-line**
  In the **Command-line** tab, enter the **Destination disk (-DST)**.
  You must enter the details of the destination of the Mac client computer where the image is to be deployed. The format to enter the destination is **diskname:partition or volume number**.
  To know the disk name and partition details of the Mac source computer, navigate to **Go > Utilities > Terminal** and enter the command `diskutil list`.
  On executing the command, the details of the Mac client computer are displayed. For example, disk0s1, disk0s2, disk2s1 and so on. Here for disk0s1, disk0 is the disk name and 1 is the partition number or the volume number.
  In Deployment Solution, the **Destination disk (-DST)** field starts with 1, here 1 corresponds to the disk 0 of the Mac computer. Similarly 2 corresponds to disk 1 of the Mac computers and so on.

Following are few examples of the disk name and partition number format that should be entered in the **Destination disk**

(-DST) field.

- For disk0s2 specify the value as 1:2, where 1 is the disk name and 2 is the partition number.
- For disk1s2 specify the value as 2:2, where 1 is the disk name and 2 is the partition number.
- For disk2s1 specify the value as 3:1, where 3 is the disk name and 1 is the partition number.
- For disk2s2 specify the value as 3:2, where 3 is the disk name and 2 is the partition number.

See “Creating and deploying Mac images” on page 165.

See “Creating a Mac image” on page 168.

Appendix A

Troubleshooting

This appendix includes the following topics:

- About Symantec Notification Manager
- Installing the Symantec Management Agent for Mac
- Launching the Symantec Management Agent for Mac GUI
- Using the Symantec Management Agent for Mac GUI

About Symantec Notification Manager

Symantec Notification Manager is an application that displays administrative alerts before it runs a task or restarts the computer. Symantec Notification Manager is a part of the Symantec Management Agent for Mac. ()

For example, the Notification Server computer administrator can create a software installation task that requires the computer to be restarted. Before it restarts the computer, Symantec Notification Manager displays an alert. The alert asks the currently logged-in user to close all programs.

If you miss an alert, you can open Symantec Notification Manager. To open the manager, click **Active Alerts** in the Symantec Management Agent for Mac GUI and view the list of active alerts for all users. (See "Using the Symantec Management Agent for Mac GUI" on page 176.)

Installing the Symantec Management Agent for Mac

The Notification Server computer administrator installs the Symantec Management Agent for Mac. To install the Symantec Management Agent for Mac refer to your Notification Server documentation.

Launching the Symantec Management Agent for Mac GUI

You can launch the Symantec Management Agent for Mac graphical user interface (GUI) on the Mac computer. Navigate to /Applications/Utilities/ and open the Symantec Management Agent application.

You can drag the Symantec Management Agent icon into the Dock for convenient access.

Using the Symantec Management Agent for Mac GUI

The Symantec Management Agent for Mac graphical user interface (GUI) contains the following sections:

- Agent Details
- Special Periods
- Software Management
- Task Management

Each GUI section includes several options.

Table A-1 Options in the Agent Details section

Option	Description
General	The General group displays the following Symantec Management Agent information: ■ The Notification Server computer address with which the Symantec Management Agent for Mac is registered. ■ The version of Notification Server software. ■ The unique identifier of the Macintosh computer. This identifier is used to register the computer with Notification Server. The Client Configuration group displays the following information: ■ The last time the Symantec Management Agent for Mac requested a client configuration file from Notification Server. ■ The last time an updated client configuration file was received. ■ How often the Symantec Management Agent for Mac should query Notification Server for a new client configuration file. The client configuration policy defines this parameter. (For more information, see the *Notification Server User Guide*.) To request the client configuration manually, click **Refresh Now**. The **Basic Inventory** group displays the following information: ■ The last time that the Symantec Management Agent sent the computer identification information to Notification Server. Computer information includes hardware and software inventory. ■ Basic inventory send interval, as defined by the client configuration policy. (For more information, see the *Notification Server User Guide*.) To send basic inventory manually, click **Send Now**.

Table A-1 Options in the Agent Details section *(continued)*

Option	Description
Plug-ins	Displays the Symantec Management Agent for Mac plug-ins that are registered on the managed Macintosh computer. Displays the plug-in version and installation directory.
Policies	Displays the client configuration policies that apply to the managed Macintosh computer, as defined by the Notification Server computer administrator. To request configuration policies from the server, click **Refresh Configuration Now**. To view details of the configuration policy, click **Show Details**.
Active alerts	Click to launch the Symantec Notification Manager application. This application displays the active alerts that precede administrative task execution and computer restarts. See "About Symantec Notification Manager" on page 175.
Log Viewer	Click to launch the console application and view the Symantec Management Agent for Mac log. The default log level is **error**. For information about changing the log level, see the *Notification Server User Guide*.

Table A-2 Options in the Special Periods section

Option	Description
Maintenance windows	Displays the maintenance windows, as defined by the Notification Server computer administrator. When maintenance windows are defined, tasks can be run only within the specific periods of time. For more information, see the *Notification Server User Guide*.

Table A-2 Options in the Special Periods section *(continued)*

Option	Description
Network blockouts	Displays the network communication blockouts, as defined by the Notification Server computer administrator. When a network communication blockout is active, network traffic between the Symantec Management Agent and Notification Server is reduced. For more information, see the *Notification Server User Guide*.
Bandwidth throttling	Displays the network bandwidth throttling settings, as defined by the Notification Server computer administrator. When bandwidth throttling is enabled, the bandwidth that the Symantec Management Agent for Mac uses is limited. For more information, see the *Notification Server User Guide*.

Table A-3 Option in the Software Management section

Option	Description
Software Delivery	Displays the Software Management Solution tasks that are available for the managed Macintosh computer. To check if any new tasks are available for this computer, click **Refresh Tasks from Server**. To view details of available tasks, or to run or suspend a task, click **Show Details**. For more information, see the Software Management Solution user guide .

Table A-4 Options in the Task Management section

Option	Description
Client Task Agent	The Connectivity group shows the task server with which the Client Task Agent is registered. It also shows the connection status of the Client Task Agent. To force registration with the task server, click **Register**. The Client Tasks group shows the number of active tasks that are assigned to this managed Macintosh computer by the task server. To check if any new tasks are available for this computer, click **Check for New Tasks**. For more information, see the Task Server user guide .
Client Tasks	Displays the list of tasks that are assigned to this managed Macintosh computer by the task server. To manually check if any new tasks are available, click **Check for New Tasks**. To view finished tasks, click **Show Tasks History**.

Index

A

about configuration
  Symantec Management Agent for Mac computers 56
agent registration policy
  creating 31
agent registration request
  allowing 44
  blocking 44
agent registration status
  report 44
agent settings for Mac computers
  Agent Settings tab
    Installation Settings dialog box 53
agent trust
  about 22
  accept 31
  block 31
  establishing 22
  registration policy 31
  revoking 44
agent-based inventory 68
applicability check
  about 95

B

basic inventory 67
basic inventory data 67

C

checking agent installation
  Mac installation prerequisites 44
command-line options
  managing Mac client computers 48
compliance
  checking 114
compliance check
  about 95
components
  Software Management Solution 90
computer
  pulling Symantec Management Agent for UNIX, Linux, and Mac 43
  pushing Symantec Management Agent for UNIX, Linux, or Mac 40
configuration
  Symantec Management Agent for Mac computers 57
Connection and Authentication tab
  Installation Settings dialog box 49
CSV file
  importing Mac computers 28, 30
Custom inventory 69
custom inventory
  gathering 76
  process 76
  viewing data for a data class 85
custom inventory data 69

D

data class
  viewing inventory data 85
deploying Symantec Management Agent to Mac OS X client computer
  Mac installation prerequisites 39
disabling or configuring built-in Mac OS X firewall
  Mac installation prerequisites 35
discovering Mac computers 17
  Network Discovery wizard 18
  with manually created tasks 19
DMG file
  creating to deliver software to Mac OS X computers 104

F

filescan.rule file
  about 82
  customizing 82
  using to scan for files on Mac computers 83

H

home page 119
hosting an internal SUS
about 113

I

implementation
Software Management Solution 92
implementing
Patch Management Solution for Mac 112
incoming connections to Mac computers
through Secure Shell (SSH) 33
installation prerequisites for Mac agent and plug-ins 23
checking agent installation 44
deploying Symantec Management Agent to Mac OS X client computer 39
disabling or configuring built-in Mac OS X firewall 35
setting up Notification Server name resolution 34
installation settings
Symantec Management Agent for UNIX, Linux, and Mac 38
Installation Settings dialog box 38
Agent Settings tab for Mac computers 53
Connection and Authentication tab 49
login and password settings 51
platform detection settings 53
SSH authorization settings 50
SSH password authorization settings 50
timeout settings 52
Install XML tab for Mac computers 55
installer
importing into the Software Catalog
to deliver software to Mac OS X computers 105
Installer Shell script
creating
to deliver software to Mac OS X computers 105
installing Mac agent and plug-ins 26
about 21
installing Mac computers with pull (manual) agent installation 43
internal Software Update Server (SUS)
about hosting to obtain internal software updates 113
inventory
managed computers 74
methods 67
inventory data
methods for gathering 67
viewing in reports 84
viewing in Resource Manager 85
Inventory for Mac
About Inventory Solution 65
inventory on Mac computers
gathering 66
process 66
Inventory Plug-in
checking deployment on Mac computers 71
installing 69
inventory policies
predefined 72
inventory policy
creating and configuring 74
inventory reports 84
Inventory Solution
information gathered with a policy
checking 76
information gathered with a task
checking 87
troubleshooting Mac problems 70, 86
Inventory Solution policy
troubleshooting Mac problems 75
inventory task
creating and configuring 74
inventorying computers 114

K

key CMS Mac capabilities and limitations
compared to Windows 12

L

local Software Update Server (SUS)
redirecting a Mac client computer 116
login and password settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 51
login settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 51

M

Mac agent and plug-ins
about 48
installation prerequisites 23
installing 21, 26

Mac client computer
redirecting to a local Software Update Server (SUS) 116
Mac client computers
about selecting for Symantec Management Agent pull (manual) installation 30
creating CSV file for computer details 28
managing with command-line options 48
selecting for Symantec Management Agent pull (manual) installation 30
Mac computers 90
See also UNIX, Linux, and Mac
about managing with CMS 12
key CMS capabilities and limitations 12
supported package-delivery formats 14
about software inventory using the filescan.rule file 82
about supported package-delivery formats 14
checking deployment of the Inventory Plug-in 71
checking the inventory information that is gathered with policies 76
checking the inventory information that is gathered with tasks 87
configuring maintenance window 60
configuring software delivery tasks 102
configuring Symantec Management Agent policies 56–57
discovering 17
discovering with tasks created manually 19
discovering with tasks using the wizard 18
enabling devnote logging for troubleshooting 87
ensuring that Mac computers can receive the Inventory Solution policy 75
global agent settings 57
installing the Inventory Plug-in 70
key CMS capabilities and limitations 12
sample task, creating a DMG file to deliver software 104
sample task, creating a Managed Software Delivery policy to deliver software to Mac OS X computers 108
sample task, creating a task to disable the Product Improvement pop-up 107
sample task, creating an Installer Shell script to deliver software 105
sample task, importing an installer into the Software Catalog to deliver software 105
scanning using the filescan.rule file 83
support in Software Management Solution 90
Mac computers *(continued)*
targeted agent settings 58
troubleshooting problems using devnote logging 87
troubleshooting problems with Inventory Solution 86
using tasks to manage 101
Mac OS X client computer
checking agent installation 44
deploying Symantec Management Agent 39
Mac OS X firewall
disabling or configuring 35
Mac software
how patching works 113
Mac Terminal 22, 33
See also Secure Shell (SSH)
maintenance window
configuring policy 60
Managed Software Delivery
actions 99
compliance. *See* compliance check
key tasks 99
policy creation 100
remediation. *See* remediation, software
wizard 100
managing Mac computers with CMS
about 12

N

Network Discovery 18–19
process 17–18
task 19
wizard 17
Network Discovery task
creating 18–19
location 18–19
modifying 19
Network Discovery wizard 18–19
Notification Server name resolution
Mac installation prerequisites 34

O

options, Software Management Solution. *See* settings, Software Management Solution

P

password authorization settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 50
password settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 51
Patch Management Solution for Mac
about 111
implementing 112
return codes 120
patching Mac software
about 114
See also Patch Management Solution for Mac
how it works 113
See also Patch Management Solution for Mac
platform detection settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 53
platform support, Software Management Solution 90
policy
global agent settings 57
maintenance window policy 60
targeted agent settings 58
policy to deliver software to Mac OS X computers
creating 108
portal
Software Portal. *See* Software Portal
portal page 119
predefined inventory policies
cloning 72
using 72
prerequisites
Symantec Management Agent for Mac
installation 23

R

remediation, software
about 95
reports
viewing 119
Resource Manager
viewing inventory data 85
return codes
patch management for Mac 120

S

Secure Shell (SSH) 22, 33
See also Mac Terminal
authorization settings 50
password authorization settings 50
security
Software Management Solution 93
selecting Mac computers for pull (manual) agent installation 30
settings, Software Management Solution
default 93
task. *See* task options, Software Management Solution
software delivery
advanced 99
methods 96
software delivery tasks for Mac computers
configuring 102
software inventory
filescan.rule file on managed Mac computers 82
Software Management Solution 93, 96
See also settings, Software Management Solution
See also Software Portal
components 90
delivering Mac software 90
implementing 92
key tasks 91
Software Portal 96
See also software request
about 96
Software Update Server (SUS)
about hosting 113
redirecting a Mac client computer 116
software updates
obtaining by hosting an internal SUS 113
viewing available 115
viewing installation status 119
solution plug-ins for Mac computers
about 48
specifying agent installation settings
Symantec Management Agent for Mac computers 38
SSH Key authorization settings
Connection and Authentication tab
Installation Settings dialog box 50
standard inventory data 68
supported package-delivery formats
for Mac software distribution in CMS 14
SUS. *See* Software Update Server

Symantec Management Agent
configuring agent policies for Mac 56
importing Mac computers from CSV file 28, 30
selecting Mac computers for installation 30
Symantec Management Agent for Mac
about configuring for Mac computers 56
configuring agent policies for Mac 57
configuring for Mac computers 57
configuring maintenance window policy 60
global settings 57
installation settings
Install Settings dialog box 38
local settings 58
selecting computers for installation 30
specifying installation settings 38
targeted settings 58
Symantec Management Agent for Mac 7.1
about Symantec Notification Manager 175
installing 175
launching the GUI 176
using the GUI 176
Symantec Management Agent for UNIX, Linux, and Mac
installation settings
specifying 38
Symantec Management Agent for UNIX, Linux, or Mac
CSV template file 28
importing computers from CSV file 28, 30
installation requirements 23
installation settings 38
agent execution settings 53
agent settings 53
agent settings, preserving 53
authentication settings 49
command timeout setting 52
configuration 55
connection settings 49
login and password 51
login settings 51
login timeout setting 52
package upload speed setting 52
password settings 51
platform detection settings 53
privileged user account settings 51
SSH password authorization settings 50
startup 55
unprivileged user account settings 51
upgrade 55
upgrade, configuration, and startup 55
Symantec Management Agent for UNIX, Linux, or Mac *(continued)*
installation settings *(continued)*
XML format for manual installation 55
installation settings, Agent Settings tab 53
installation settings, Connection and Authentication tab 49
login and password settings 51
platform detection settings 53
SSH key authorization settings 50
SSH password authorization settings 50
timeout settings 52
installation settings, Install XML tab 55
installing on Mac computers 21, 26
installing on selected computers 40
installing with a pull (manually) 43
Mac installation prerequisites 23
prerequisites 23
pulling from the console to Mac computers 43
push installation process 40
pushing to computers 40
selecting computers for installation 30
simultaneous installation tasks, setting 40
Symantec Notification Manager
about 175

T

task options, Software Management Solution
about 94
task settings, Software Management Solution. *See* task options, Software Management Solution
task to disable the Product Improvement pop-up
creating 107
task, Software Management Solution
options. *See* task options, Software Management Solution
settings, default 93
tasks
using to manage Mac computers 101
timeout settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 52
troubleshooting
Mac problems with Inventory Solution 70–71, 75–76, 86–87

U

UNIX, Linux, and Mac
    support in Software Management Solution 90
updating computers
    checking needed updates 114
    viewing available updates 115
    viewing status reports 119
updating Mac software. *See* patching Mac software
upgrade, configuration, and startup settings for Mac computers
    Install XML tab for Mac computers
        Installation Settings dialog box 55